Document made available under the Patent Cooperation Treaty (PCT)

International application number: PCT/JP04/018491

International filing date: 10 December 2004 (10.12.2004)

Document type: Certified copy of priority document

Document details: Country/Office: JP
Number: 2004-261033
Filing date: 08 September 2004 (08.09.2004)

Date of receipt at the International Bureau: 10 February 2005 (10.02.2005)

Remark: Priority document submitted or transmitted to the International Bureau in compliance with Rule 17.1(a) or (b)

PCT/JP2004/018491

13.12.2004

日　本　国　特　許　庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出　願　年　月　日
Date of Application:　２００４年　９月　８日

出　願　番　号
Application Number:　特願２００４－２６１０３３

[ST. 10/C]:　［Ｊ Ｐ ２００４－２６１０３３］

出　願　人
Applicant(s):　松下電器産業株式会社

２００５年　１月２８日

特許庁長官
Commissioner,
Japan Patent Office　小　川　洋

出証番号　出証特２００５－３００４１２７

【書類名】　特許願
【整理番号】　2054061310
【提出日】　平成16年 9月 8日
【あて先】　特許庁長官殿
【国際特許分類】　H04L 9/08
H04L 29/06
H04N 5/91
【発明者】
【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内
【氏名】　森岡　芳宏
【特許出願人】
【識別番号】　000005821
【氏名又は名称】　松下電器産業株式会社
【代理人】
【識別番号】　100097445
【弁理士】
【氏名又は名称】　岩橋　文雄
【選任した代理人】
【識別番号】　100103355
【弁理士】
【氏名又は名称】　坂口　智康
【選任した代理人】
【識別番号】　100109667
【弁理士】
【氏名又は名称】　内藤　浩樹
【手数料の表示】
【予納台帳番号】　011305
【納付金額】　16,000円
【提出物件の目録】
【物件名】　特許請求の範囲　1
【物件名】　明細書　1
【物件名】　図面　1
【物件名】　要約書　1
【包括委任状番号】　9809938

出証特２００５－３００４１２７

【書類名】特許請求の範囲
【請求項１】
送信手段と受信手段の間でデータのパケット通信を行なうパケット送受信系において、
　ＡＶデータの入力端子種別の検出手段と、
　前記ＡＶデータと非ＡＶデータとをそれぞれ入力するデータ入力手段と、
　前記非ＡＶデータまたは前記ＡＶデータの少なくとも一方より前記ＡＶデータの属性情報を検出し、前記ＡＶデータの暗号化モード情報を生成する手段と、
　前記データ入力手段の出力を入力し、規定の送受信条件により「暗号化または暗号化情報ヘッダー付加の実行を行う」暗号化データ生成手段と、
　パケットヘッダー付加手段とを具備するパケット送受信手段において、
　前記暗号化データ生成手段は認証手段と暗号化手段と暗号化情報ヘッダー付加手段を具備し、
　前記規定の送受信条件により前記暗号化手段において暗号化を実行するかしないか、および、前記暗号化情報ヘッダー付加手段において暗号化情報ヘッダー付加を行うか行わないかを制御する手段と
　前記ＡＶデータの入力端子種別の検出手段により検出され判別された入力端子種別情報と前記ＡＶデータの属性情報の少なくとも一方の情報を用いて、前記送信手段と前記受信手段の間での前記ＡＶデータの伝送プロトコルを決定する手段を具備するパケット送信装置。
【請求項２】
前記暗号化データ生成手段内の前記暗号化手段は暗号化に際して暗号化鍵を使用し、前記送信手段と前記受信手段が規定の条件を具備していることを検証し認証が行われた後に暗号化鍵が前記送信手段と前記受信手段で共有され、規定の伝送条件により前記暗号化鍵が更新されることを特徴とする請求項１記載のパケット送信装置。
【請求項３】
前記暗号化データ生成手段内の認証手段において、
前記送信手段と前記受信手段との間で認証を実行するモードと認証を実行しないモードを持ち、どちらのモードにおいても前記暗号化情報ヘッダー付加手段において前記暗号化モード情報を用いて暗号化情報ヘッダーを付加することを特徴とする請求項２記載のパケット送信装置。
【請求項４】
前記認証手段において認証を実行するモードは、前記外部より入力される制御情報により決定することを特徴とする請求項３記載のパケット送信装置。
【請求項５】
前記外部より入力される制御情報または認証用のＴＣＰポート情報は、コンテンツ毎にアクセス位置を指定するＵＲＩ、または、Ｑｕｅｒｙにより拡張されたＵＲＩ情報とにより与えられることを特徴とする請求項４記載のパケット送信装置。
【請求項６】
前記外部より入力される制御情報または認証用のＴＣＰポート情報は、コンテンツ毎にアクセス位置を指定するＵＲＩで要求されたコンテンツの情報の返信時に与えることを特徴とする請求項４記載のパケット送信装置。
【請求項７】
前記認証手段において認証を実行するモードは、
　前記入力ＡＶデータより抽出した制御情報より決定することを特徴とする請求項３記載のパケット送信装置。
【請求項８】
前記認証手段において認証を実行するモードは、
前記外部より入力される制御情報および前記入力ＡＶデータの双方により決定することを特徴とする請求項３記載のパケット送信装置。
【請求項９】

前記ＡＶデータに関するコピー制御情報により前記暗号化情報ヘッダーを付加するかどうかを決定するヘッダー付加制御手段を具備することを特徴とする請求項３から８記載のパケット送信装置。
【請求項１０】
前記ＡＶデータがコピーフリーコンテンツを放送する放送チャネルを受信したコンテンツの場合、または、前記ＡＶデータが蓄積メディアよりコピーフリータイトルのコンテンツを再生した場合には、前記暗号化情報ヘッダーを付加せず、
前記ＡＶデータが一定期間でもコピーフリーでないコンテンツを放送する放送チャネルを受信したコンテンツの場合、または、前記ＡＶデータが蓄積メディアよりコピーフリーでないタイトルのコンテンツを再生した場合には、前記暗号化情報ヘッダーを付加することを特徴とする請求項９記載のパケット送信装置。
【請求項１１】
前記コピーフリーコンテンツを放送する放送チャネルは、アナログ放送であるVHF、UHF、またはＢＳアナログ放送の放送チャネルであることを特徴とする請求項１０記載のパケット送信装置。
【請求項１２】
前記一定期間でもコピーフリーでないコンテンツを放送する放送チャネルのコピー制御情報は、コピーネバー、コピーワンジェネレーション、およびＥＰＮフラグ付きコピーフリーのうち少なくとも１つのモードを含んでいることを特徴とする請求項１０記載のパケット送信装置。
【請求項１３】
前記一定期間でもコピーフリーでないコンテンツを放送する放送チャネルは、デジタル放送であるBSデジタル放送、地上波デジタル放送、またはＣＳデジタル放送の放送チャネルであることを特徴とする請求項１０記載のパケット送信装置。
【請求項１４】
前記一定期間でもコピーフリーでないコンテンツを放送する放送チャネルの受信は、前記放送の配信を行う事業者との間での認証手段により正当な受信装置または受信ユーザであることを認証された場合に行われることを特徴とする請求項１３記載のパケット送信装置。
【請求項１５】
前記認証は、日本のデジタル衛生放送のB-CADカード、または米国のＣＡＴＶ放送で使用されるPODカードなどのセキュリティモジュールによる認証であることを特徴とする請求項１４記載のパケット送信装置。
【請求項１６】
前記暗号化手段は前記暗号化情報ヘッダーを、前記ＡＶデータがフリーコンテンツの場合には付加しない、または、前記ＡＶコンテンツの意味のあるデータ単位毎に付加することを特徴とする請求項３から８記載のパケット送信装置。
【請求項１７】
ＡＶデータと非ＡＶデータとをそれぞれのデータバッファに入力し、前記２つのバッファの出力は優先制御して前記パケットヘッダー付加手段に出力することを特徴とする請求項１から１６記載のパケット送信装置。
【請求項１８】
前記優先制御の方法は、前記非ＡＶデータが前記データバッファでオーバーフローしない様に制御しながら、前記ＡＶデータを前記データバッファから優先して出力することを特徴とする請求項１７記載のパケット送信装置。
【請求項１９】
前記前記ＡＶデータの伝送プロトコルでＴＣＰプロトコルを用いる場合は、ＴＣＰコネクションを永続的接続にすることを特徴とする請求項１から１８記載のパケット送信装置。
【請求項２０】
前記暗号化鍵を共有するための認証と鍵交換方式は、ＤＴＣＰ方式であることを特徴とす

る請求項１から１９記載のパケット送信装置。
【請求項２１】
前記暗号化鍵のＩＤ情報または更新情報として整数値を前記暗号化情報ヘッダーまたはパケットヘッダーに付加することを特徴とする請求項２０記載のパケット送信装置。
【請求項２２】
パケットヘッダー付加手段から出力されるパケットをＨＴＴＰプロトコルで伝送する場合、ＨＴＴＰパケットのパケット毎に、前記整数値はランダム値または特定の規則に基づく更新値に更新することを特徴とする請求項２１記載のパケット送信装置。
【請求項２３】
パケットヘッダー付加手段から出力されるパケットをＨＴＴＰプロトコルで伝送する場合、ＴＣＰプロトコルが切断して再コネクションを張る毎に、前記整数値はランダム値または特定の規則に基づく更新値に更新することを特徴とする請求項２１記載のパケット送信装置。
【請求項２４】
前記暗号化モードの変化はＴＣＰプロトコルまたはＵＤＰプロトコルのポート番号の変化で検出して設定することを特徴とする請求項２０記載のパケット送信装置。
【請求項２５】
前記暗号化モードの情報をパケット内に持つことを特徴とする請求項２０記載のパケット送信装置。
【請求項２６】
前記ＡＶデータのパケット化は、ＲＴＰ、ＵＤＰ、ＩＰプロトコルで行うことを特徴とする請求項１から２５記載のパケット送信装置。
【請求項２７】
前記暗号化鍵の更新条件としては、あらかじめ決められた時間ごとに行うという条件も用いることを特徴とする請求項２６記載のパケット送信装置。
【請求項２８】
前記ＡＶデータのパケット化は、ハードウエアで行うことを特徴とする請求項２６記載のパケット送信装置。
【請求項２９】
マルチキャスト伝送の場合、前記暗号化情報ヘッダーを付加したパケットと付加しないパケットの両方を出力することを特徴とする請求項２６記載のパケット送信装置。
【請求項３０】
前記ＡＶデータを前記ＲＴＰ、ＵＤＰ、ＩＰプロトコルによるＩＰパケット化の前に、フォーワードエラーコレクション（ＦＥＣ）による誤り訂正を付加することを特徴とする請求項２６記載のパケット送信装置。
【請求項３１】
前記フォーワードエラーコレクション（ＦＥＣ）はリードソロモン方式またはパリティ方式であることを特徴とする請求項２６記載のパケット送信装置。
【請求項３２】
前記暗号化情報ヘッダーを付加する場合は、前期ＲＴＰプロトコルにおいて定義されているマーカービット（Ｍビット）を有効状態にアサートすることを特徴とする請求項２６記載のパケット送信装置。
【請求項３３】
前記ＡＶデータのパケット化は、ＨＴＴＰ、ＴＣＰ、ＩＰプロトコルで行うことを特徴とする請求項１から２５記載のパケット送信装置。
【請求項３４】
前記パケット化において、ＨＴＴＰプロトコルはチャンク伝送方式で行ない、ＨＴＴＰパケットのペイロード長を前記送信手段で決定して伝送することを特徴とする請求項３３記載のパケット送信装置。
【請求項３５】

前記ＨＴＴＰパケットのペイロード長は、前記暗号化情報ヘッダー長と前期ＡＶデータを構成するＴＳまたはタイムスタンプつきＴＳの整数倍値を加算した長さであることを特徴とする請求項３４記載のパケット送信装置。
【請求項３６】
前記パケット化において、前記ＨＴＴＰは前記受信手段からのレンジリクエストまたはデータ取得コマンドを受けて前記ＡＶデータまたは前記暗号化モード情報のうち少なくとも一方を含んだペイロードデータを伝送することを特徴とする請求項３３記載のパケット送信装置。
【請求項３７】
前記レンジリクエストまたはデータ取得コマンドは、前記送信側における前記ＡＶデータがＭＰＥＧの場合、ＭＰＥＧストリームにおける不連続発生連続性情報、前記ＡＶデータのファイル内におけるＭＰＥＧのＩピクチャーまたはＰピクチャーまたはＢピクチャーの位置情報、前記ＭＰＥＧのＩピクチャーまたはＰピクチャーまたはＢピクチャーの時刻情報、或るＩピクチャーから次のＩピクチャーの間に存在するＰピクチャとＢピクチャーの各個数または合計個数の内、少なくとも１つの情報を参照して実行することを特徴とする請求項３６記載のパケット送信装置。
【請求項３８】
前記ＡＶデータのファイル内におけるＭＰＥＧのＩピクチャーまたはＰピクチャーまたはＢピクチャーの位置情報または時刻情報は、前記ＡＶデータが複数の異なるファーマットであった場合にもオリジナルに持っている複数のＩピクチャーまたはＰピクチャーまたはＢピクチャーの位置情報または時刻情報より、複数の異なるファーマット間で共通なＩピクチャーまたはＰピクチャーまたはＢピクチャー位置情報または時刻情報を生成し、この共通のＩピクチャーまたはＰピクチャーまたはＢピクチャー位置情報または時刻情報を用いて前記ＡＶデータのファイル内におけるＭＰＥＧのＩピクチャーまたはＰピクチャーまたはＢピクチャーの位置情報または時刻情報の参照情報とすることを特徴とする請求項３７記載のパケット送信装置。
【請求項３９】
前記ＡＶデータのパケット化は、受信側のＡＶデータ出力がディスプレイ充てに出力されて蓄積されない場合はＲＴＰが用い、受信側のＡＶデータ出力が記録メディアに蓄積される場合はＨＴＴＰを用いられる様に、受信側からの制御により、ＲＴＰまたはＨＴＴＰプロトコルで行うことを切替え制御することを特徴とする請求項２６または３３記載のパケット送信装置。
【請求項４０】
前記ＡＶデータは、ＳＭＰＴＥ　２５９Ｍ規格で規定された非圧縮ＳＤ方式信号、または、ＳＭＰＴＥ　２９２Ｍ規格で規定された非圧縮ＨＤ形式、または、ＩＥＣ　６１８８３規格で規定されたＩＥＥＥ１３９４によるＤＶまたはデジタル放送のＭＰＥＧ－ＴＳの伝送ストリーム形式、または、ＤＶＢ規格Ａ０１０で規定されたＤＶＢ－ＡＳＩによるＭＰＥＧ－ＴＳ形式、または、ＭＰＥＧ－ＰＥＳ，ＭＰＥＧ－ＥＳ、ＭＰＥＧ４、ＩＳＯ／ＩＥＣ　Ｈ．２６４の内のいずれか一つのデータストリーム形式を含むことを特徴とする請求項２６から３９記載のパケット送信装置。
【請求項４１】
前記ＡＶデータを構成するデータブロックにタイムスタンプを付加し、１つ以上のタイムスタンプ付データブロックをまとめてＲＴＰまたはＨＴＴＰ上にマッピングすることを特徴とする請求項４０記載のパケット送信装置。
【請求項４２】
前記ＡＶデータがＭＰＥＧ－ＴＳの場合、各ＴＳパケットにタイムスタンプを付加し、複数のタイムスタンプ付ＴＳパケットをまとめてＲＴＰまたはＨＴＴＰ上にマッピングすることを特徴とする請求項４１記載のパケット送信装置。
【請求項４３】
前記各ＴＳパケットに付加するタイムスタンプのクロックはＭＰＥＧのシステムクロック

周波数に等しいことを特徴とする請求項４２記載のパケット送信装置。
【請求項４４】
前記ＴＳパケットに付加されたタイムスタンプより、ＭＰＥＧ－ＴＳのネットワーク伝送によりＰＣＲに付加した伝送ジッターを除去して、受信側でのＭＰＥＧシステムクロックの再生を行うことを特徴とする請求項４３記載のパケット送信装置。
【請求項４５】
Ｎを２以上の整数とした場合、ＵＤＰプロトコルまたはＴＣＰプロトコルのＮ個のポートを用いて、Ｎ個のフォーマットのＡＶデータをそれぞれのポート毎に割り当てて伝送することを特徴とする請求項４０記載のパケット送信装置。
【請求項４６】
ＵＤＰプロトコルまたはＴＣＰプロトコルの単一のポートを用いて、複数のフォーマットのＡＶデータを多重して伝送することを特徴とする請求項４０記載のパケット送信装置。
【請求項４７】
Ｎを２以上の整数、また、ＭをＮより大きい整数とした場合、ＵＤＰプロトコルまたはＴＣＰプロトコルのＭ個のポートを用いて、Ｎ個のフォーマットのＡＶデータを単一または多重してＭ個のポートに割り当てて伝送することを特徴とする請求項４０記載のパケット送信装置。
【請求項４８】
複数のＡＶデータを同時に伝送する場合、高データレートのＡＶデータはＵＤＰプロトコルで伝送し、低データレートのＡＶデータはＴＣＰプロトコルで伝送することを特徴とする請求項４０記載のパケット送信装置。
【請求項４９】
複数のＡＶデータを同時に伝送する場合、高データレートのＡＶデータより、低データレートのＡＶデータを優先して伝送することを特徴とする請求項４０記載のパケット送信装置。
【請求項５０】
前記ＡＶデータの伝送範囲を制限することを特徴とする請求項２６から３記載のパケット送信装置。
【請求項５１】
前記ＡＶデータの伝送範囲を制限は、ＩＰプロトコルのＴＴＬ（Ｔｉｍｅ　ｔｏ　Ｌｉｖｅ）の値を用いて制限することを特徴とする請求項５０記載のパケット送信装置。
【請求項５２】
前期前記ＡＶデータの伝送範囲を制限は、ＩＰパケットのＲＴＴ（Ｒｏｕｎｄ　Ｔｒｉｐ　Ｔｉｍｅ）の値を用いて制限することを特徴とする請求項５０記載のパケット送信装置。
【請求項５３】
前記ＡＶデータの伝送範囲を制限は、ＭＡＣ層のヘッダー情報により制限することを特徴とする請求項５０記載のパケット送信装置。
【請求項５４】
前記ＩＰパケットのパケットサイズは前期送信手段と受信手段の間のＩＰネットワークのパスＭＴＵサイズ以下に設定することを特徴とする請求項２６から３９記載のパケット送信装置。
【請求項５５】
前記ＩＰパケットの伝送は、ＩＥＥＥ　８０２．３で規定された伝送方法により行われることを特徴とする請求項２６から３９記載のパケット送信装置。
【請求項５６】
前記ＩＰパケットの伝送は、ＩＥＥＥ　８０２．１１で規定された伝送方法により行われることを特徴とする請求項２６から３９記載のパケット送信装置。
【請求項５７】
前記ＩＥＥＥ　８０２．１１の使用において、ＷＥＰまたはＷＰＡまたはその他のネット

ワーク接続制限手段を用いることを特徴とする請求項５６記載のパケット送信装置。
【請求項５８】
前記ＩＰパケットの伝送は、ＩＥＥＥ　８０２．１Ｑにより規定された伝送方法により行われることを特徴とする請求項２６から３９記載のパケット送信装置。
【請求項５９】
前記ＩＰパケットの伝送は、ＩＰバージョン４、または、ＩＰバージョン６を使用して行われることを特徴とする請求項２６から３９記載のパケット送信装置。
【請求項６０】
前記ＩＰバージョン４を用いる場合、ＴＯＳフィールドを用いて優先制御を行なうことを特徴とする請求項５７記載のパケット送信装置。
【請求項６１】
前記ＩＰバージョン６を用いる場合、Ｐｒｉｏｒｉｔｙフィールドを用いて優先制御を行なうことを特徴とする請求項５９記載のパケット送信装置。

【書類名】明細書
【発明の名称】パケット送信装置
【技術分野】
【０００１】
本発明は、ＩＥＥＥ　８０２．３などのイーサネット（登録商標）（有線ＬＡＮ）やＩＥＥＥ　８０２．１１などの無線ＬＡＮなどを用いて、暗号化されたＡＶストリームをＩＰパケット化して高品質に送信するパケット送信装置に関する。
【背景技術】
【０００２】
従来、一般家庭において、ＩＥＥＥ　１３９４を用いて、ＩＥＣ　６１８８３－４で規定された方式に基づきＭＰＥＧ－ＴＳ信号の暗号化伝送が行なわれている。ＭＰＥＧ－ＴＳなどＡＶデータを暗号化して伝送する方式の一例として、ＤＴＣＰ（Digital Transmission Content Protection）方式が規定されている。ＤＴＣＰは、ＩＥＥＥ　１３９４やＵＳＢなどの伝送メディア上のコンテンツ保護技術である。ＤＴＣＰ方式は、ＤＴＬＡ(Digital Transmission Licencing Administrator)で規格化された方式であり、 HYPERLINK "http://www.dtcp.com" http://www.dtcp.com、 HYPERLINK "http://www.dtcp.com/data/dtcp#tut.pdf" http://www.dtcp.com/data/dtcp#tut.pdf、HYPERLINK "http://www.dtcp.com/data/wp#spec.pdf" http://www.dtcp.com/data/wp#spec.pdfや、書籍「ＩＥＥＥ１３９４、ＡＶ機器への応用」、高田信司監修、日刊工業新聞社、「第８章、コピープロテクション」、１３３～１４９ページで説明されている。
【０００３】
図９は、ＤＴＣＰ方式を用いたＭＰＥＧ―ＴＳのＩＥＥＥ　１３９４での伝送の一例である。ＤＴＣＰ方式では、送信側をソース９０１、受信側をシンク９０２と呼び、暗号化したＭＰＥＧ－ＴＳなどのコンテンツをソース９０１からネットワーク９０３を介して、シンク９０２へ伝送している。なお、図９に、補足情報として、ソース機器およびシンク機器の例を併記する。
【０００４】
次に、図１０を用いて、ＤＴＣＰ方式における従来のパケット通信手段の概略を説明する。図１０は図９のソース９０１、およびシンク９０２の構成の概略図である。まず、ＤＴＣＰ方式に準拠した認証と鍵交換（Authentification and Key Exchange、ＡＫＥと略する）が行なわれる。ＡＫＥ手段１００１に対して、その認証と鍵交換設定情報が入力され、この情報がパケット化手段１００２により規定のヘッダーを付加されパケット化され、ネットワーク１００７に出力される。ここで、パケット化手段１００２は送信条件設定手段１００３により決定された送信パラメータにより、入力データのパケット化および送信を行なう。受信側では、ネットワーク１００７より入力する信号がパケット受信手段１００４でパケットヘッダーなどの識別によりフィルタリングされ、ＡＫＥ手段１００１に入力される。これにより送信側（ソース）のＡＫＥ手段と、受信側（シンク）のＡＫＥ手段がネットワーク１００７（図９においてはネットワーク９０３）を介してお互いにメッセージの通信ができる。すなわち、ＤＴＣＰ方式の手順に従い、認証と鍵交換を実行する。
【０００５】
送信側（ソース）と、受信側（シンク）で認証と鍵交換が成立すれば、次に、ＡＶデータの伝送を行なう。ソースでは、ＭＰＥＧ－ＴＳ信号を暗号化手段１００５に入力して、ＭＰＥＧ－ＴＳ信号を暗号化した後、この暗号化されたＭＰＥＧ－ＴＳ信号をパケット化手段１００２に入力し、ネットワーク１００７に出力する。シンクでは、ネットワーク１００７より入力する信号がパケット受信手段１００４でパケットヘッダーなどの識別によりフィルタリングされ、復号手段１００６に入力され、復号されＭＰＥＧ－ＴＳ信号が出力される。
【０００６】
次に、図１１を用い上記手順を補足説明する。図１１において、ソースとシンク間はＩ

ＥＥＥ　１３９４で接続されている。まず、ソース側でコンテンツの送信要求が発生する。そして、ソースからシンクへ暗号化されたコンテンツおよびコンテンツの保護モード情報が送信される。シンクは、コンテンツのコピー保護情報の解析を行い、完全認証もしくは制限付き認証のどちらの認証方式を用いるかを決定し、認証要求をソースに送る。ソースとシンクはＤＴＣＰ所定の処理により認証鍵の共有を図る。そして、ソースは認証鍵を用いて交換鍵を暗号化してシンクに送り、シンクで交換鍵が復号される。ソースでは暗号鍵を時間的に変化させるために、時間的に変化するシード情報を生成し、シンクに送信する。ソースでは、交換鍵とシード情報より暗号化鍵を生成して、ＭＰＥＧ－ＴＳをこの暗号化鍵を用いて暗号化手段で暗号化してシンクに送信する。シンクはシード情報を受信し交換鍵とシード情報より復号鍵を復元する。シンクではこの復号鍵を用いて暗号化されたＭＰＥＧ－ＴＳ信号を復号する。

【０００７】

図１２は、図１０においてＭＰＥＧ－ＴＳ信号を伝送する場合のＩＥＥＥ　１３９４アイソクロナスパケットの一例である。このパケットは、４バイト（３２ビット）のヘッダー、４バイト（３２ビット）のヘッダーＣＲＣ、２２４バイトのデータフィールド、４バイト（３２ニット）のトレイラによって構成されている。暗号化されて伝送されるのは２２４バイトのデータフィールドを構成するＣＩＰヘッダーとＴＳ信号のうち、ＴＳ信号のみで、他のデータは暗号化されない。ここで、ＤＴＣＰ方式固有の情報は、コピー保護情報である２ビットのＥＭＩ（Encription Mode Indicator）、およびシード情報のＬＳＢビットであるＯ／Ｅ（Odd/Even）であり、これらは上記３２ビットのヘッダー内に存在するため暗号化されずに伝送される。

【特許文献１】特開２０００－５９４６３号公報

【発明の開示】

【発明が解決しようとする課題】

【０００８】

しかしながら、上記従来の構成では以下のような問題点を有していた。従来のＤＴＣＰ方式はＩＥＥＥ　１３９４において、アイソクロナスパケットを用いて伝送するためＭＰＥＧ－ＴＳ信号のリアルタイム伝送ができるが、インターネットの標準プロトコルであるＩＰプロトコルを用いて、イーサネット（登録商標）（ＩＥＥＥ　８０２．３）、無線ＬＡＮ（ＩＥＥＥ　８０２．１１）や、その他のＩＰパケットを伝送可能なネットワークで伝送ができないという大きな問題点がある。

【０００９】

すなわち、ＩＰプロトコルを介して論理的に接続された送信機器と受信機器の間を、地上波／ＢＳデジタル放送やサーバー型放送などデジタル著作権保護対応のコンテンツを著作権保護しつつ伝送できないという大きな問題点がある。

【００１０】

また、ライブ放送の伝送において、ＨＴＴＰプロトコルを用いる場合、ＨＴＴＰリクエストの度に、前記暗号化に関して付加するヘッダー長や伝送コンテンツ長を受信側で計算する必要があり、受信側の処理が重いという課題がある。

【００１１】

さらに、ハードディスクなどに蓄積されたコンテンツを早送り、巻き戻し、スロー再生などの特殊再生の簡単に実現することが困難であるという問題点がある。

【００１２】

さらに、ハードディスクや光ディスクなどに蓄積された異なる蓄積フォーマットのコンテンツを共通の方法で簡単に、早送り、巻き戻し、スロー再生などの特殊再生することが困難であるという問題点がある。

【課題を解決するための手段】

【００１３】

上記課題を解決するために、本願第１の発明は、課金処理などを含むＲＭＰなどのデジタル著作権対応のＡＶデータおよび非ＡＶデータとをそれぞれ入力するデータ入力手段と

、前記データ入力手段の出力を入力し、入力されるデジタル著作権規定より暗号化伝送モードを選択できる手段を具備する。すなわち、「暗号化または暗号化情報ヘッダー付加の実行を行う」暗号化データ生成手段と、パケットヘッダー付加手段とを具備するパケット送受信手段において、前記暗号化データ生成手段は認証手段と暗号化手段と暗号化情報ヘッダー付加手段を具備し、前記規定の送受信条件により前記暗号化手段において暗号化を実行するかしないか、および、前記暗号化情報ヘッダー付加手段において暗号化情報ヘッダー付加を行うか行わないかを制御する手段とを具備する。

【００１４】

これにより、課金処理などを含むＲＭＰ情報などデジタル著作権対応のＭＰＥＧ－ＴＳ信号などのＡＶストリームを外部から与えられる一定規則による送信条件に従い暗号化モードを決め、さらに暗号化情報ヘッダーを付加することを決めることにより、送受信機器間での信号の互換性を確保しながら、ＡＶストリームの秘匿性を保つことが可能となる。

【００１５】

本願第２の発明は、第１の発明において、ライブで放送されているコンテンツをＨＴＴＰのチャンク伝送方式で伝送することにより、前記暗号化に関して付加するヘッダー長や伝送コンテンツ長ＨＴＴＰリクエストの度に、受信側（クライアント）で計算する必要がなくなり、受信側の処理を軽くすることができる。

【００１６】

本願第３の発明は、第１の発明において、ハードディスクなどに蓄積されたコンテンツをＨＴＴＰのレンジリクエストを用いて伝送することにより、早送り、巻き戻し、スロー再生などの特殊再生を簡単に実現することができる。

【００１７】

さらに、本願第４の発明は、第３の発明において、ハードディスクや光ディスクなどに蓄積された異なる蓄積フォーマットのコンテンツの異なるＩ、Ｐ、Ｂピクチャのバイト位置情報、時刻情報より、共通フォーマットとしてのＩ、Ｐ、Ｂピクチャフレーム位置情報を生成することにより、高品質なスロー再生、早送り、巻き戻しなどの特殊再生を容易に実現することが可能となる。

【発明の効果】

【００１８】

本願第１の発明によれば、以下のような効果を有する。すなわち、地上波放送、衛星放送、ＣＡＴＶやインターネット経由で受信するデジタル放送信号より検出、抽出できるＡＶコンテンツの属性情報を送信端末と受信端末間でＵＰｎＰ－ＡＶやＨＴＴＰなどのデータ交換プロトコルを用いて伝送することにより、送信端末と受信端末間でのＡＶコンテンツを送信する場合の暗号化モード、コンテンツ属性情報の伝送方法を決めることができる。さらに、暗号化情報ヘッダーの付加ルールを決められるため、送受信機器間でのＡＶストリームの秘匿性を保ちながら信号の互換性を確保することが可能となる。

【００１９】

また、本願発明によれば、ネットワークを用いたＡＶコンテンツの伝送に関して、ネットワーク上でのデータ盗聴を防止し、安全性の高いデータ伝送を実現する。これにより、伝送路にインターネットなど公衆網を使用した場合においても、リアルタイム伝送される優先データ（ＡＶデータコンテンツ）の盗聴、漏洩を防止することができる。また、インターネット等で伝送されるＡＶデータの販売、課金が可能となり、安全性の高いＢ－Ｂ、Ｂ－Ｃのコンテンツ販売流通が可能となる。

【００２０】

また、本願発明によれば、ＡＶコンテンツをハードウェアで伝送処理する場合にも、一般のデータパケットは従来通りＣＰＵを用いてソフトウェア処理を行える。よって、ソフトウェアの追加により管理情報や制御情報などデータを一般データとして伝送させることができる。これらのデータ量は優先データであるＡＶデータに比べて非常に少ないので、マイコンなど安価なマイクロプロセッサーで実現可能となり低コストなシステムを実現することができる。なお、高負荷かつ高伝送レート優先パケットのプロトコル処理にも高価

なＣＰＵや大規模メモリを必要としないので、これらの点からも低コストで高機能な装置を提供できる。

【００２１】

そこで、本願発明によれば、サーバー型放送のＲＭＰで用いる課金情報などを含むＲＭＰＩで視聴あるいはコピー制限されたコンテンツをＲＭＰに対応していないクライアントにＣＮＭ（Ｃｏｐｙ　Ｎｏ　Ｍｏｒｅ）やＣＮ（Ｃｏｐｙ　Ｎｅｖｅｒ）で見せることができ、サーバー型放送の普及を加速することができる。

【００２２】

本願第２の発明によれば、以下のような効果を有する。すなわち、ライブで放送されているコンテンツをＨＴＴＰのチャンク伝送方式で伝送することにより、前記暗号化に関して付加するヘッダー長や伝送コンテンツ長ＨＴＴＰリクエストの度に、受信側（クライアント）で計算する必要がなくなり、受信側の処理を軽くできる。

【００２３】

本願第２の発明によれば、以下のような効果を有する。すなわち、ハードディスクなどに蓄積されたコンテンツをＨＴＴＰのレンジリクエストを用いて伝送することにより、早送り、巻き戻し、スロー再生などの特殊再生を簡単に実現できる。

【００２４】

さらに、本願第４の発明は、第３の発明において、ハードディスクや光ディスクなどに蓄積された異なる蓄積フォーマットのコンテンツの異なるＩフレーム位置情報より、共通のＩフレーム位置情報を生成することにより、簡単に、早送り、巻き戻し、スロー再生などの特殊再生することを実現する。

【発明を実施するための最良の形態】

【００２５】

最初に本願発明の位置付けを明確にするために適用されるシステム例の概略について説明する。図１は本願発明を適用するシステムの一例である。

【００２６】

図１において、送信機器１０１および受信機器１０３は、本願第１，２，３、４および５の発明実施部である（以下、本願発明部）。１０１は送信機器、１０２はルータ、１０３は受信機器である。送信機器１０１には、送受信条件の設定情報、認証と鍵交換の設定情報、入力ストリーム（ＭＰＥＧ－ＴＳなどコンテンツ）が入力され、以下の手順１から３に基づき、通信が実行される。

【００２７】

＜手順１＞送受信パラメータの設定を行なう。

【００２８】

（手順１－１）送受信機器のＭＡＣアドレス、ＩＰアドレス、ＴＣＰ／ＵＤＰポート番号等を設定。

【００２９】

（手順１－２）送信信号の種別、帯域を設定。ＱｏＳエージェントとして動作する送信機器１０１と受信機器１０３、ＱｏＳマネージャとして動作するルータ１０２との間でＩＥＥＥ　８０２．１Ｑ（ＶＬＡＮ）規格を用いたネットワークの運用に関する設定を実施。

【００３０】

（手順１－３）優先度の設定（ＩＥＥＥ　８０２．１Ｑ／ｐによる運用）

＜手順２＞認証と鍵交換：

（手順２－１）認証と鍵交換を行なう。たとえば、ＤＴＣＰ方式を用いることもできる。

【００３１】

＜手順３＞ストリーム伝送：

（手順３－１）送信機器と受信機器間での暗号化されたストリームコンテンツ（ＭＰＥＧ－ＴＳ）の伝送

なお、コンテンツの入力信号としてＭＰＥＧ１／２／４などにおけるＭＰＥＧ－ＴＳ，ＭＰＥＧ－ＰＳ、ＭＰＥＧ－ＥＳ、ＭＰＥＧ－ＰＥＳなどがある。

【００３２】

ここでは、例ではＭＰＥＧ－ＴＳを使用しているが、これに限らず本発明で用いる入力コンテンツの適用範囲としては、ＭＰＥＧ１／２／４などＭＰＥＧ－ＴＳストリーム（ＩＳＯ／ＩＥＣ　１３８１８）、ＤＶ（ＩＥＣ　６１８３４、ＩＥＣ　６１８８３）、ＳＭＰＴＥ　３１４Ｍ（ＤＶ－ｂａｓｅｄ）、ＳＭＰＴＥ　２５９Ｍ（ＳＤＩ）、ＳＭＰＴＥ　３０５Ｍ（ＳＤＴＩ）、ＳＭＰＴＥ　２９２Ｍ（ＨＤ－ＳＤＩ）等で規格化されているストリーム、さらには、一般的なＡＶコンテンツも適用可能である。

【００３３】

さらに、本発明で用いる入力データの適用範囲として、データのファイル転送にも適用可能である。ファイル転送の場合、送受信端末の処理能力と送受信端末間の伝播遅延時間の関係により、データ転送速度がコンテンツストリームの通常再生データレートよりも大きくなるなどの条件化において、リアルタイムより高速のコンテンツ伝送も可能である。

【００３４】

次に、上記手順２の認証と鍵交換に関して補足説明する。図２において、送信機器と受信機器間はＩＰネットワークにより接続されている。まず、送信機器から受信機器へコンテンツのコピー保護情報を含んだコンテンツの保護モード情報が送信される。

【００３５】

受信機器は、コンテンツのコピー保護情報の解析を行い、使用する認証方式を決定して認証要求を送信機器に送る。

【００３６】

これらの処理を通して送信機器と受信機器は認証鍵を共有する。

【００３７】

次に、送信機器は認証鍵を用いて交換鍵を暗号化して受信機器に送り、受信機器で交換鍵が復号される。

【００３８】

送信機器では暗号鍵を時間的に変化させるために、時間的に変化する鍵変更情報を生成し、受信機器に送信する。

【００３９】

送信機器では、交換鍵と鍵変更情報より暗号化鍵を生成して、ＭＰＥＧ－ＴＳをこの暗号化鍵を用いて暗号化手段で暗号化して受信機器に送信する。

【００４０】

受信機器は受信した鍵変更情報を交換鍵より復号鍵を復元する。受信機器ではこの復号鍵を用いて暗号化されたＭＰＥＧ－ＴＳ信号を復号する。

【００４１】

図３は本方式をイーサネット（登録商標）を用い２階建ての家庭に適用した場合の一例である。

【００４２】

図３において、３０１は１階のネットワーク構成、３０２は２階のネットワーク構成である。

【００４３】

３０３は１階に設置されインターネットと接続されるルータ、３０４は２階に設置されているスイッチングハブである。

【００４４】

３０４はルータ３０３とスイッチングハブ３０４を接続するイーサネット（登録商標）ネットワークである。家庭内の全てのイーサネット（登録商標）ネットワークの帯域は１００Ｍｂｐｓである。

【００４５】

１階のネットワーク構成の詳細としては、ルータ３０３にはテレビ（ＴＶ）、パソコン

（ＰＣ）、ＤＶＤレコーダが１００Ｍｂｐｓのイーサネットで接続され、また、エアコン、冷蔵庫がＥＣＨＯＮＥＴで接続されている。

【００４６】

また、２階では、スイッチングハブ３０４にテレビ（ＴＶ）、パソコン（ＰＣ）、ＤＶＤレコーダが１００Ｍｂｐｓのイーサネットで接続され、また、エアコンがＥＣＨＯＮＥＴで接続されている。なお、ＥＣＨＯＮＥＴは「エコーネットコンソーシアム」（HYPERLINK "http://www.echonet.gr.jp/" http://www.echonet.gr.jp/）で開発されている伝送方式である。

【００４７】

図３において、パソコン（ＰＣ）、ＤＶＤレコーダ、ルータ３０１およびスイッチングハブ（３０４）は、ＩＥＥＥ　８０２．１Ｑ（ＶＬＡＮ）に対応している。すなわち、ルータ（３０１）およびスイッチングハブ（３０４）において、各ポートのデータレートが全て同じ（例えば１００Ｍｂｐｓ）場合、特定ポートへ出力されるデータ帯域の合計がそのポートの伝送レートの規格値または実力値を超えない限り、入力ポートへ入力されたデータはルータ（あるいは、スイッチングハブ）内部で失われず全て出力ポートに出力される。

【００４８】

スイッチングハブでは、たとえば８個の入力ポートにデータが同時に入力されても、それぞれのデータの出力ポートが異なっていれば、それぞれのデータはハブ内部のバッファで競合しないでスイッチングされて出力ポートより出力されるため、入力データはパケット落ちすることなく全て出力ポートに出力される。

【００４９】

図３において、家庭内の全てのイーサネット（登録商標）の帯域が１００Ｍｂｐｓであるため、１階と２階間のネットワーク３０５の帯域も１００Ｍｂｐｓである。

【００５０】

１階と２階の複数の機器間で複数のデータが流れる場合、各データに対する帯域制限がない場合、このネットワーク３０５上を流れるデータのデータレート合計が１００Ｍｂｐｓを超える可能性があり、ＭＰＥＧ－ＴＳの映像アプリなどリアルタイム伝送が必要なストリームが途切れる可能性がある。

【００５１】

この場合、リアルタイム伝送が必要なストリームが途切れない様にするには、伝送データに対して優先制御が必要である。

【００５２】

端末だけでなく、ルータやスイッチングハブにおいて、後述するストリーム伝送やファイル転送の速度制限機構などを導入することにより解決できる。

【００５３】

たとえば、ＭＰＥＧ－ＴＳストリームの伝送優先度をファイル転送データの伝送優先度よりも高くすると、１階と２階のＰＣ間でのファイル転送をバックグラウンドで行いながら、同時に、１階および２階のＤＶＤレコーダ、ＰＣ，ＴＶの間でＭＰＥＧ－ＴＳを暗号化してリアルタイムで伝送することが可能となる。

【００５４】

前述したルータ、またはスイッチングハブにおける伝送速度制限機構は、データ流入制御により実現できる。

【００５５】

すなわち、ルータ（あるいは、スイッチングハブ）の入力データキューにおいて優先度の高いデータと低いデータを比較して、優先度の高いデータを優先して出力することにより実現できる。

【００５６】

この優先制御方式に用いるバッファ制御ルールとしては、ラウンドロビン方式、流体フェアスケジューリング方式、重み付けフェアスケジューリング方式自己同期フェアスケジ

ューリング方式ＷＦＦＱ方式、仮想時計スケジューリング方式、クラス別スケジューリング方式などがある。

【００５７】

これらのスケジューリング方式に関する情報は、戸田巌著、「ネットワークＱｏＳ技術」、平成１３年５月２５日（第１版）、オーム社刊の第１２章などに記述されている。

【実施例１】

【００５８】

本願第１の発明について説明する。図４は本願第１の発明のパケット送受信手段に関するブロック図である。

【００５９】

４０１は入力ＡＶコンテンツをその関連メタ情報が持つ送信条件に従う暗号化、関連メタ情報の付加、パケット化を行うパケット送受信手段である。

【００６０】

ここで、送信条件設定管理手段４０３には、送信データのフォーマット種別、送信先アドレスやポート番号などの送信情報、送信に用いるパス情報（ルーティング情報）、送信データの帯域、送信データの送信優先度などの送信条件の設定情報、送信手段（ローカル）と受信手段（リモート）における機器の管理制御データと、受信状況を送信側にフィードバックするためのデータが入力される。

【００６１】

コンテンツはその選択に関して、コンテンツ毎または放送チャネル毎にＱｕｅｒｙにより拡張されたＵＲＩ情報で与える。ここで、ＵＲＩに主データ部にコンテンツのＵＲＩ情報、Ｑｕｅｒｙ部にそのコンテンツの認証情報をマッピングする。これにより、もし、Ｑｕｅｒｙ部がなければそのコンテンツの伝送には認証が不必要であり、Ｑｕｅｒｙ部が存在すればそのコンテンツの伝送には認証が必要である様にモード設定することができる。ＵＲＩとＱｕｅｒｙの例は、例えば下記の形式で与えることができる。

【００６２】

＜ｓｅｒｖｉｃｅ＞：／／＜ｈｏｓｔ＞：＜ｐｏｒｔ＞／＜ｐａｔｈ＞／＜ｆｉｌｅｎａｍｅ＞．＜ｅｘｔ＞？ＡＫＥＰＯＲＴ＝＜ｐｏｒｔ２＞

ここで、＜ｈｏｓｔ＞：＜ｐｏｒｔ＞／＜ｐａｔｈ＞／＜ｆｉｌｅｎａｍｅ＞．＜ｅｘｔ＞はＡＶコンテンツのＵＲＩとファイル名称を表しており、以下のＱｕｅｒｙ部における＜ｐｏｒｔ２＞は認証用ポート番号を表わす。ここで、一般に認証サーバーとコンテンツ提供サーバーが同一であれば、認証用ポートのＩＰアドレスはＡＶコンテンツのＩＰアドレスと同じであるが、認証サーバーとコンテンツ提供サーバーが異なる場合には認証用ポートのＩＰアドレスはＡＶコンテンツのＩＰアドレスと異なる。送信側はこれら、ＵＲＩとＱｕｅｒｙで認証の実行モード情報を受信側に与える。受信側はＷＥＢブラウザやＵＰｎＰ－ＡＶのＣＤＳ（コンテンツディレクトリサービス）を用いて、上記のＵＲＩとＱｕｅｒｙ情報を受け取り、認証モードを決定することができる。

【００６３】

また、ＤＲＭ設定管理手段４０４は、送信条件の設定管理手段４０３またはＴＳストリーム識別手段よりＤＲＭ設定情報を受け取り、その情報を保持、管理するとともに、ＡＫＥに必要な関連情報をＡＫＥ手段４０５に引き渡す。ここで、ＤＲＭはDigital Rights Managementの略であり、デジタル著作権管理のことである。ＤＲＭ設定管理手段で、コンテンツ伝送にはＤＲＭの課金、購入処理が必要な場合にはＤＲＭコンテンツ購入手段（４１１）によりコンテンツの購入処理が行われる。コンテンツの購入処理が終了後に、コンテンツのＣＣＩ（コピー制御情報）が設定されＡＫＥ手段４０５に渡される。

【００６４】

ここで、ＡＫＥは、「認証と鍵交換」（Authentification and Key Exchange）の略語であり、ＡＫＥ手段は認証手段と暗号化鍵の交換手段を具備する。

【００６５】

ＡＫＥ手段４０５に対してＡＫＥ設定情報を入力し、このＡＫＥ設定情報に関連した情

報、たとえばコピー保護情報と暗号化鍵変更情報、がパケット化手段４０６に入力され、ＴＣＰ／ＩＰプロトコルのヘッダーを付加され、さらに、フレーム化手段４０８においてＭＡＣ（Ｍｅｄｉａ　Ａｃｃｅｓｓ　Ｃｏｎｔｒｏｌ）ヘッダーが付加されイーサネット（登録商標）フレームに変換し、送信フレームとしてネットワークに出力される。

【００６６】

図４を用いて、ＤＴＣＰ方式による著作権対応のＡＶコンテンツの伝送ステップの一例について説明する。ここで、ＤＲＭ対応のＡＶコンテンツとはデジタル放送のコピー制御や、サーバー型放送（ＡＲＩＢ規格、ＳＴＤ－Ｂ３８）のＲＭＰ方式（ＲＭＰＩ）や、各種のネットワークＤＲＭで扱っているコンテンツ保護情報を表す。

【００６７】

（ステップ１）まず、受信側で送信側より、ＵＰｎＰ－ＡＶ、ＣＤＳ（Content Directory service)などで与えられるコンテンツリストより受信したいコンテンツを選択し、ソース側にコンテンツの送信要求を投げる。

【００６８】

（ステップ２）コピー制御情報またはＤＲＭ情報を含んだデータがＴＳストリーム識別手段４０２により抽出され、ＤＲＭ設定管理手段４０４経由で、ＡＫＥ手段４０５に入力される。

【００６９】

ＤＴＣＰ情報としてはＡＫＥ手段４０５よりコンテンツの保護モード情報（ＥＭＩ情報）が暗号化情報ヘッダー付加手段４１５に出力され、ヘッダー情報として付加された後、パケット化手段４０６に入力される。

【００７０】

（ステップ３）受信側（シンク）では、パケット受信手段４１０よりＡＫＥコマンド受信処理を行うＡＫＥ手段４０５に入力されたコンテンツのコピー保護情報の解析を行い、完全認証もしくは制限付き認証のどちらの認証方式を用いるかを決定し、認証要求をソースに送る。

【００７１】

（ステップ４）ソースとシンク間でＤＴＣＰ所定の処理が行なわれ、認証鍵が共有される。

【００７２】

（ステップ５）次に、ソースはＡＫＥ手段４０５において、認証鍵を用いて交換鍵を暗号化してパケット化手段４０６を経由してシンクに送り、シンクのＡＫＥ手段において交換鍵が復号される。

【００７３】

（ステップ６）ソースでは暗号鍵を時間的に変化させるために、暗号化鍵生成手段において、時間的に変化するシード情報（Ｏ／Ｅ）を生成し、ＡＫＥ手段４０５、暗号化情報ヘッダー付加手段４１５、およびパケット化手段４１６を経由してシンクに送信する。

【００７４】

（ステップ７）ソースでは、暗号化鍵を生成するＡＫＥ手段４０５において交換鍵とシード情報より暗号化鍵を生成して、暗号化手段でＭＰＥＧ－ＴＳを暗号化してパケット化手段４０６に出力する。

【００７５】

（ステップ８）シンク内部の、暗号鍵変更情報を生成するＡＫＥ手段４０５はパケット受信手段４１０よりシード情報を受信し、復号鍵を生成するＡＫＥ手段４０５はこのシード情報と交換鍵より復号鍵を復元する。

【００７６】

（ステップ９）シンクでは、この復号鍵を用いて復号化手段４１８において、暗号化されたＭＰＥＧ－ＴＳ信号入力を復号して出力する。

【００７７】

ここで、ＤＲＭコンテンツがあって、そのコピー可能回数がＮ回（Ｎは２以上の整数）

である場合の動作について説明する。まず、受信端末がＤＲＭに対応している場合には、伝送暗号状態のＣＣＩをＣＯＧ（コピー１回可能）またはＣＮＭ（コピーノーモア）、またはＣＮ（コピーネバー）に設定して伝送する。

【００７８】

ここで、暗号化伝送されるエンベデッドＣＣＩとして「残りのコピー可能回数情報」を（Ｎ－１）回として受信側に伝え、受信側で暗号を復号した後に、ＤＲＭ対応端末では残りのコピー可能回数を（Ｎ－１）回に設定する。

【００７９】

また、受信端末がＤＲＭに対応していない場合には、コンテンツのＤＲＭ情報は削除してＮＭＣのＣＣＩを用いて受信側に伝送する。

【００８０】

図４において、ＡＫＥ手段は暗号化ヘッダー情報を暗号化情報ヘッダー付加手段４１５に入力し、以下の様に暗号化情報ヘッダー付加制御を行なう。

【００８１】

図４において、送信条件の設定管理手段４０３に入力されるＡＶデータの関連情報（放送、または蓄積コンテンツ再生の場合）は、たとえば次のような場合が考えられる。

（ケース１）　前記ＡＶデータがコピーフリーコンテンツを放送する放送チャネルを受信したコンテンツの場合。この様な放送チャネルの例としては、たとえば、アナログ放送であるＶＨＦ、ＵＨＦ、またはＢＳアナログ放送の放送チャネルがある。

（ケース２）前記ＡＶデータが一定期間でもコピーフリーでないコンテンツを放送する放送チャネルを受信したコンテンツの場合。この様な放送チャネルの例としては、たとえば、ＢＳデジタル放送の有料チャネルやＣＡＴＶ放送による有料チャネルがある。この一定期間でもコピーフリーでないコンテンツを放送する放送チャネルのコピー制御情報は、コピーネバー、コピーワンジェネレーション、およびＥＰＮフラグ付きコピーフリーが放送内容により時々刻々と切り替わるのが特徴である。

ここで、一定期間でもコピーフリーでないコンテンツを放送する放送チャネルの受信は、前記放送の配信を行う事業者との間での認証手段により正当な受信装置または受信ユーザであることを認証された場合に行われるように制御できる。この認証の例としては、日本のデジタル衛星放送のＢ－ＣＡＳカード、または米国のＣＡＴＶ放送で使用されるＰＯＤカードなどのセキュリティモジュールによる認証が考えられる。

【００８２】

また、暗号化情報ヘッダーの付加制御は、たとえば以下の様に行なう。すなわち、コピーフリーコンテンツを放送する放送チャネルを受信した場合には付加しない。

【００８３】

また、一定期間でもコピーフリーでないコンテンツを放送する放送チャネルを受信した場合には付加する。さらに、ＡＶデータが蓄積メディアよりコピーフリータイトルのコンテンツを再生した場合には付加しない。

【００８４】

そして、ＡＶデータが蓄積メディアよりコピーフリーでないタイトルのコンテンツを再生した場合には付加する。

【００８５】

以上の様に、暗号化情報ヘッダーの付加制御を行うことにより、著作権者が設定したＡＶコンテンツのＣＣＩ（コピー制御情報）をネットワーク伝送においても継承して伝えていくことができる。

【００８６】

さらに、送信側と受信側で暗号化情報ヘッダーの付加制御のルールを揃えることにより異機種間での動作互換性を確保することができる。

【００８７】

ここで、パケット化手段４０６は送信条件の設定管理手段４０３により決定された送信パラメータにより、入力データのパケット化および送信を行なう。

【００８８】
送信条件の設定管理手段４０３は、送信キュー制御手段４０７に、送信先アドレスやポート番号などの送信情報、送信に用いるパス情報（ルーティング情報）、送信データの帯域、送信データの送信優先度などの送信条件を与える。
【００８９】
これらのデータは、ＴＣＰ／ＩＰ処理によるパケット化手段４０６およびフレーム化手段４０８で生成するヘッダーやペイロードデータなどを設定する。
【００９０】
受信側では、ネットワークより入力する信号がフレーム受信手段４０９でＭＡＣヘッダーを元にフィルタリングされ、ＩＰパケットとしてパケット受信手段４１０に入力される。パケット受信手段４１０ではＩＰパケットヘッダーなどの識別によりフィルタリングを行い、ＡＫＥ手段４０５に入力される。これにより送信側のＡＫＥ手段と、受信側のＡＫＥ手段がネットワークを介して接続されるので、通信プロトコルを介してお互いにメッセージの交換ができる。すなわち、ＡＫＥ手段の設定手順に従い、認証と鍵交換を実行することができる。
【００９１】
送信側と、受信側で認証と鍵交換が成立すれば、暗号化したＡＶデータを送信する。
【００９２】
送信側では、入力信号が例えばＭＰＥＧのフルＴＳストリームの場合、そのフルＴＳストリームをＴＳストリーム識別手段４０２に入力し、フルＴＳストリームをパーシャルＴＳストリームに変換する。
【００９３】
そして、変換されたパーシャルＴＳストリームをコンテンツバッファ４１３に送り暗号化タイミングの調整を行う。
【００９４】
コンテンツバッファ４１３のパーシャルＴＳ出力を暗号化手段４１４に入力し暗号化を行ない、前述したＥＭＩ、シード情報（シード情報のすべてのビット、または、Ｏ／Ｅなど一部のビット）などのＡＫＥ情報を暗号化情報ヘッダー付加手段４１５で付加する。
【００９５】
さらに、この信号をパケット化手段４０６に入力し、送信キュー制御手段４０７より与えられる条件を用いてＴＣＰ／ＩＰプロトコルのヘッダーを付加する。パケットの優先伝送制御を行うためには、フレーム化手段４０８において、たとえば、８０２．１Ｑ（ＶＬＡＮ）方式を用いて、ＭＡＣヘッダーを付加しイーサネット（登録商標）フレームに変換して、送信フレームとしてネットワークに出力する。ここで、ＭＡＣヘッダー内のＴＣＩ（Tag Control Information）内のＰｒｉｏｒｉｔｙ（ユーザ優先度）を高く設定することにより、ネットワーク伝送の優先度を一般のデータよりも高くすることができる。
【００９６】
受信側では、ネットワークより入力する信号がフレーム受信手段４０９でＭＡＣヘッダーを元にフィルタリングされ、ＩＰパケットとしてパケット受信手段４１０）入力される。パケット受信手段４１０でパケットヘッダーなどの識別によりフィルタリングし、送信条件などの伝送関連データは送信条件の条件設定手段４１７に出力し、ＡＫＥ関連データはＡＫＥ手段４０５に出力し、ＡＶコンテンツは暗号の復号化手段４１８に出力する。復号化手段４１８では、暗号化情報ヘッダーの除去と暗号の復号化が行われ、復号されたＭＰＥＧ－ＴＳ信号が出力される。
【００９７】
なお、送信条件設定手段４１７には、受信状況を送信側にフィードバックするためのデータが入力され、ＩＰパケットのパケット化手段４０６およびイーサネット（登録商標）フレームのフレーム化手段４０８で生成するヘッダーおよびペイロードデータを設定する情報を送信条件の設定管理手段４０３にフィードバックする。
【００９８】

次に、図５のプロトコルスタックを用い上記手順を補足説明する。図５の送信側において、まず送信側から受信側へ暗号化されたコンテンツおよび、ＤＲＭ設定管理手段より与えられるコンテンツの保護モード情報が送信される。受信側は、コンテンツのコピー保護情報の解析を行い、認証方式を決定し、認証要求を送信機器に送る。次に、乱数を発生させ、この乱数を所定の関数に入力し、交換鍵を作成する。交換鍵の情報を所定の関数に入力し、認証鍵を生成する。受信側でも所定の処理により認証鍵の共有を図る。なお、ここで用いる暗号化情報としては、たとえば、送信側の独自情報（機器ＩＤ、機器の認証情報、マックアドレスなど）、秘密鍵、公開鍵、外部から与えられた情報などを１つ以上組み合わせて生成した情報であり、ＤＥＳ方式やＡＥＳ方式など暗号化強度の強い暗号化方式を用いることにより強固な暗号化が可能である。そして、送信側は認証鍵を用いて交換鍵を暗号化して受信側に送り、受信側で交換鍵が復号される。また、交換鍵と初期鍵更新情報を所定の関数に入力し、暗号化鍵を生成する。なお、送信側では暗号鍵を時間的に変化させるために、時間的に変化する鍵更新報を生成し、受信側に送信する。コンテンツであるＭＰＥＧ－ＴＳは暗号化鍵により暗号化される。そして暗号化されたＭＰＥＧ－ＴＳは、ＡＶデータとしてＴＣＰ（またはＵＤＰ）パケットのペイロードとしてＴＣＰパケットが生成される。さらにこのＴＣＰパケットはＩＰパケットのデータペイロードとして使用され、ＩＰパケットが生成される。さらにこのＩＰパケットはＭＡＣフレームのペイロードデータとして使用され、イーサネット（登録商標）ＭＡＣフレームが生成される。なお、ＭＡＣとしてはイーサネット（登録商標）であるＩＥＥＥ　８０２．３だけでなく、無線ＬＡＮ規格のＩＥＥＥ　８０２．１１のＭＡＣにも適用できる。

【００９９】

さて、イーサネット（登録商標）ＭＡＣフレームは、イーサネット（登録商標）上を送信側から受信側へ伝送される。受信側で所定の手順に従って復号鍵を生成する。そして、受信したイーサネット（登録商標）ＭＡＣフレームからＩＰパケットがフィルタリングされる。さらにＩＰパケットからＴＣＰ（またはＵＤＰ）パケットが抜き出される。そして、ＴＣＰ（またはＵＤＰ）パケットからＡＶデータが抜き出され、交換鍵と鍵変更情報より復元された復号鍵により、ＭＰＥＧ－ＴＳ（コンテンツ）が復号され出力される。

【０１００】

以上、ＭＰＥＧ－ＴＳ信号などのＡＶストリームを送信機器で暗号化して、ＩＰパケットをネットワークにより伝送し、受信機器で元の信号に復号できる。

【０１０１】

なお、図４においては、送信キュー制御手段４０７、第１キュー手段としてのＡＶデータキュー、および第２キュー手段としての一般データキューを具備している。

【０１０２】

図４において、ＡＫＥ手段４０５に対してＡＫＥ設定情報を入力され、このＡＫＥ設定情報に関連した情報（たとえば、コピー保護情報と暗号化鍵変更情報）、および、送信データの種別、送信先アドレスやポート番号の情報、送信に用いるパス情報（ルーティング情報）、送信データの帯域、送信データの送信優先度などの送信条件の設定情報と、送信手段（ローカル）と受信手段（リモート）における機器の管理制御データと、受信状況を送信側にフィードバックするためのデータがパケット化手段４０６に入力され、ＴＣＰ／ＩＰプロトコル処理をして、第１キュー手段に入力される。

【０１０３】

また、送信側ではＭＰＥＧ－ＴＳ信号を暗号化手段４１４に入力して、ＭＰＥＧ－ＴＳ信号を暗号化した後、この暗号化されたＭＰＥＧ－ＴＳ信号をパケット化手段４０６に入力し、ＴＣＰ／ＩＰプロトコル処理をして、ＡＶデータキュー手段に入力する。

【０１０４】

送信キュー制御手段４０７は、第１キューと第２キューにデータが存在する場合、どちらのデータを優先して出力するかの制御を行なう。通常状態では、一般データよりもＭＰＥＧ－ＴＳなどのコンテンツデータを優先制御して出力する。たとえば、送受信機器間でＭＰＥＧ－ＴＳを低レイテンシ（低遅延）で伝送する場合には、ＭＰＥＧ－ＴＳ用バッフ

ァも小さくなるため、オーバーフローが発生しやすい。送信側でＭＰＥＧ－ＴＳバッファがオーバーフローしそうになった場合、あるいは、受信側からフィードバックされた情報を参照して受信側のＭＰＥＧ－ＴＳのバッファがアンダーフローしそうになったことが判明した場合には、ＭＰＥＧ－ＴＳデータを優先出力する様に第２キュー手段の優先度を更に適応的に上げることにより、これらバッファ破綻を回避できる。
ただし、受信側機器（リモート機器）の再生、停止などの機器制御応答をより速くするには、第１キューの優先度を適応的に上げればよいが、これでは前述したＭＰＥＧ－ＴＳバッファのオーバーフローまたはアンダーフローが発生する可能性がある。
バッファのオーバーフローやアンダーフローを避け、かつ、受信側機器（リモート機器）の再生、停止などの機器制御応答をより速くする別手段として、機器制御用パケットだけはキューを経由せずに直接フレーム化手段に出力する方法により、迅速な制御応答が実現できる。あるいは、機器制御用パケットに対して第３キューを新たに用意する方法により、迅速な制御応答が実現できる。

【０１０５】

なお、図３において、スイッチングハブを用いたネットワークトポロジーを工夫することにより、ストリーム伝送とファイル転送を共存させることができる。

【０１０６】

たとえば、１階と２階の間のネットワーク３０５の帯域を、従来の実施例で説明した１００Ｍｂｐｓから１Ｇｂｐｓに拡張することによって、１階と２階のＰＣ間でのファイル転送をバックグラウンドで行いながら、同時に、１階および２階のＤＶＤレコーダ、ＰＣ，ＴＶの間でＭＰＥＧ－ＴＳを暗号化してリアルタイムで伝送することができる。

【０１０７】

たとえば、市販されている１００Ｍｂｐｓのポートを８つ、１Ｇｂｐｓのポートを１つ持ったスイッチングハブを用い、１階と２階を結ぶネットワーク３０５に１Ｇｂｐｓのポートを接続し、残りの８ｃｈの１００ＭｂｐｓのポートにＴＶなどのＡＶ機器を接続する。

【０１０８】

１００Ｍｂｐｓのポートは８つなので、８つのポートのデータがそれぞれ最大１００Ｍｂｐｓで入力されて１Ｇｂｐｓのポートに出力されたとしても、１００Ｍｂｐｓ×８ｃｈ＝８００Ｍｂｐｓと１Ｇｂｐｓより小さいため、８つのポートから入力されたデータはスイッチングハブ内部で失われず全て１Ｇｂｐｓのポートに出力される。よって、１階で発生したデータは全て２階に伝送することが可能である。また、逆に２階で発生したデータも全て１階に伝送することが可能である。以上の様に、スイッチングハブを用いる場合、ネットワークトポロジーを工夫することによりストリーム伝送とファイル転送を共存させることができる。

【０１０９】

また、図４のＡＫＥ手段４０５に対してＡＫＥ設定情報を入力し、このＡＫＥ設定情報に関連した情報（たとえば、コピー保護情報と暗号化鍵変更情報）、および、送信データの種別、送信先アドレスやポート番号の情報、送信に用いるパス情報（ルーティング情報）、送信データの帯域、送信データの送信優先度などの送信条件の設定情報と、送信手段（ローカル）と受信手段（リモート）における機器の管理制御データと、受信状況を送信側にフィードバックするためのデータがパケット化手段４０６に入力されプロセッサを用いた内部のソフトウェア処理でＴＣＰ／ＩＰプロトコル処理をされ、一般データキューに入力される。

【０１１０】

送信側ではＭＰＥＧ－ＴＳ信号を暗号化手段４１４に入力して、ＭＰＥＧ－ＴＳ信号を暗号化した後、この暗号化されたＭＰＥＧ－ＴＳ信号をパケット化手段４０６に入力し、内部のハードウェア処理によりＵＤＰ／ＩＰプロトコルの処理をされ、ＡＶデータキューに入力する。

【０１１１】

送信キュー制御手段４０７は、第１キューであるＡＶデータキューと第２キューである一般データキューの双方にデータが存在する場合、前述の実施の形態２と同様に、２つのキューからのデータ出力に関して優先制御を行なう。

【０１１２】

さて、受信側では、ネットワークより入力する信号がフレーム受信手段４０９でＭＡＣヘッダーを元にＩＰパケットがフィルタリングされる。ここでは、ソースの上記パケット化手段（４０６）から出力されたＩＰパケットが、シンクのパケット受信手段４１０に入力される。一般データキューで受信したパケットはプロセッサを用いたソフトウェア処理でＴＣＰ／ＩＰプロトコルの受信処理を行い、ＡＫＥ手段（４０５）または受信条件の設定管理手段４１７に出力する。また、ＡＶデータキューで受信したパケットはハードウェア処理によりＵＤＰ／ＩＰプロトコルの受信処理を行い、暗号化されたＡＶデータは復号化手段（４１８）に入力され、暗号復号を行った後にＭＰＥＧ－ＴＳを出する。

【０１１３】

なお、送信側から受信側への、ＥＭＩ、シード情報の伝送方法としては、たとえば、専用の別パケットを生成して伝送することも可能であり、暗号鍵復元がさらに困難となり、コンテンツの盗聴、漏洩をより困難にできる。インターネットなど公衆網において、リアルタイムに伝送されるＡＶデータの暗号化パラメータが変化させたり、別パケットで送ると、コンテンツの盗聴、漏洩をより困難にすることができる。管理制御データに関しては図５の例と同様に、ソフトウェア処理によりＴＣＰパケットが生成され、ＩＰパケット化される。

【０１１４】

さて、イーサネット（登録商標）ＭＡＣフレームは、イーサネット（登録商標）上を送信側から受信側へ伝送される。受信側で所定の手順に従って復号鍵を生成する。そして、受信したイーサネット（登録商標）ＭＡＣフレームからＩＰパケットがフィルタリングされる。さらにＩＰパケットからＵＤＰパケットが抜き出され、ＵＤＰパケットからＡＶデータが抜き出され、交換鍵とシード情報より復元された復号鍵Ｋｃにより、ＭＰＥＧ－ＴＳ（コンテンツ）が復号され出力される。

【０１１５】

図６は、ＭＰＥＧ－ＴＳをＩＰパケット化、さらにイーサネット（登録商標）フレーム化して伝送する場合のパケット形式の一例である。１８８バイトのＭＰＥＧ－ＴＳに６バイトのタイムコード（ＴＣ）を付加して１９４バイトの単位を作る。ＴＣは４２ビットのタイムスタンプと６ビットのベースクロックＩＤ（ＢＣＩＤ）により構成される。ＢＣＩＤによりタイムスタンプの周波数情報を表すことができる。たとえば、（ケース１）ＢＣＩＤが０ｘ００の場合は、タイムスタンプの周波数情報はない、（ケース２）ＢＣＩＤが０ｚ０１の場合は、タイムスタンプの周波数情報としては２７ＭＨｚ（ＭＰＥＧ２のシステムクロック周波数）である、（ケース３）また、ＢＣＩＤが０ｘ０２の場合は、タイムスタンプの周波数情報としては９０ｋＨｚ（ＭＰＥＧ１で使用されるクロック周波数）である、（ケース４）ＢＣＩＤが０ｘ０３の場合は、タイムスタンプの周波数情報としては２４．５７６ＭＨｚ（ＩＥＥＥ　１３９４で使用されるクロック周波数）である。（ケース５）ＢＣＩＤが０ｘ０４の場合は、タイムスタンプの周波数情報としては１００ＭＨｚ（イーサネット（登録商標）で使用される周波数）である、という様にＢＣＩＤでタイムスタンプの周波数情報を表すことができる。１９４バイト単位のデータを２つあわせて暗号化して、更に１４バイトの暗号化情報ヘッダーと合わせてＲＴＰプロトコルのペイロードとする。ここで、暗号化情報ヘッダーは、４ビットのＥＭＩと、６４ビットのシード情報と１２ビットのＲｅｓｅａｒｖｅｄ　Ｄａｔａにより構成される。ＲＴＰパケットはＵＤＰおよびＩＰプロトコルによりパケット化された後、イーサネット（登録商標）フレーム化される。イーサネット（登録商標）ヘッダとしては、図６に示す様に、標準的なイーサネット（登録商標）ヘッダとＩＥＥＥ　８０２．１Ｑ（ＶＬＡＮ）により拡張されたイーサネット（登録商標）ヘッダの両方をサポートする。なお、ＩＥＥＥ　８０２．１Ｑ（ＶＬＡＮ）により拡張されたイーサネット（登録商標）ヘッダにおけるＴＣＩフィールド

の中の３ビットのＰｒｉｏｒｉｔｙフラグにより、イーサネット（登録商標）フレームの優先度を設定することができる。

【０１１６】

以上により、送受信機器間でＭＰＥＧ－ＴＳ信号を暗号化してリアルタイム伝送が可能となるだけでなく、第２のパケット化手段がハードウェアで構成されているため、本質的にソフトウェア処理に起因する送信パケットの送り残しや受信パケットの取りこぼしが発生しない。これにより、全ての優先データパケットが完全に送信され、リアルタイム性の保証された高品質映像の伝送が可能となる。また、一般データは一時的にバッファ手段に蓄積され、優先データ伝送が優先して行なわれる中で間欠的に伝送される。また、データ量の小さい第１のパケット化手段はマイコンなど安価なプロセッサで処理できる。
さらに、ハードウェア処理により、受信処理においても、イーサネット（登録商標）フレームを受信して、３層のＩＰヘッダー、４層のＵＤＰヘッダーを同時に検査することもできる。ＭＰＥＧ－ＴＳパケットと一般データパケットを分離し、ＭＰＥＧ－ＴＳパケットの処理をハードウェアで行うことにより、受信フレームの取りこぼしが発生せず、リアルタイム性が保証された高品質な受信ができる。

【０１１７】

パケットの送信タイミング、あるいは２つの送信データキューからのデータ送信割合をソフトウェアではなくハードウェアで制御するとクロック単位で完全な送出制御が可能である。これにより全ての優先パケットが完全に送信され、リアルタイム性の保証された高品質の伝送が可能となる。また、出力パケットのシェイピングもクロック単位で正確に行われるため、初段のルータ、またはスイッチングハブでのパケット廃棄の発生確率が非常に少ない高品質な通信が可能となる。

【０１１８】

以上により、送受信機器間でＭＰＥＧ－ＴＳ信号をＤＴＣＰ方式により暗号化してリアルタイム伝送が可能となるだけでなく、第２のパケット化手段がハードウェアで構成されているため、本質的にソフトウェア処理に起因する送信パケットの送り残しや受信パケットの取りこぼしが発生しない。また、データ量の小さい第１のパケット化手段はマイコンなど安価なプロセッサで処理できる。

【実施例２】

【０１１９】

本願第２の発明について説明する。図４は本願第２の発明のパケット送受信手段に関するブロック図である。以下、第１の実施例と同じ部分の説明は省略し、異なる部分のみを説明する。

【０１２０】

本願第２の発明は、第１の発明において、ライブで放送されているコンテンツをＨＴＴＰ／ＲＴＰヘッダー付加手段４１６および、パケット化手段４０６においてＨＴＴＰのチャンク伝送方式で伝送する様に伝送プロトコルを設定する。

【０１２１】

これにより、従来は、前記暗号化に関して付加するヘッダー長や伝送コンテンツ長ＨＴＴＰリクエストの度に、受信側（クライアント）で計算していたが、この計算の必要がなくなり、受信側の処理を軽くできる。ＨＴＴＰのペイロードデータ長としては、暗号化される伝送ペイロードの暗号化情報ヘッダーとＴＳの整数倍であり、送信側で都合のよい値に設定することができる。このチャンク伝送時にはＴＣＰのコネックションは永続的接続モード（Ｋｅｅｐ　Ａｌｉｖｅ設定）されていると、ＴＣＰコネクションの切断、確立をコンテンンツ伝送中にＴＣＰトランザクション毎に頻繁に行う必要がなくなり効率のよいＡＶ伝送を行うことができる。

【実施例３】

【０１２２】

本願第３の発明について説明する。図７は本願第３の発明のパケット送受信手段に関するブロック図である。以下、第１の実施例と同じ部分の説明は省略し、異なる部分のみを

説明する。
【０１２３】
図７においては、ＴＳストリーム識別手段４０２に接続した蓄積手段７０１を具備する。ここで、蓄積手段７０１は、ハードディスクや光ディスクであり、本発明においえては、第１の発明において、ハードディスクや光ディスクなどに蓄積されたＭＰＥＧ－ＴＳデータをＨＴＴＰのレンジリクエストを用いて伝送する。
このレンジリクエストは、蓄積手段７０１に蓄積されたＭＰＥＧ－ＴＳファイルとペアになっているファイル中におけるＩフレーム位置情報を含んだファイルである。例えば、ＤＶＤ－ＶＲ方式ではＩＦＯファイルと呼ばれているものである。このＩＦＯファイルと同等のＩフレーム位置情報を持ってファイルを用いることにより、早送り、巻き戻し、スロー再生などの特殊再生を簡単に実現することができる。
【０１２４】
本発明で用いる入力データの適用範囲として、サーバー型放送や各社の異なるＤＲＭ方式など一般のＤＲＭ対応のＡＶコンテンツをＤＴＣＰ－ＩＰを用いて伝送することが可能となる。
【実施例４】
【０１２５】
本願第４の発明について説明する。図８は本願第４の発明のパケット送受信手段に関するブロック図である。以下、第３の実施例と同じ部分の説明は省略し、異なる部分のみを説明する。
【０１２６】
図７においては、蓄積手段７０１は、ハードディスクや光ディスクなどに蓄積された異なる蓄積フォーマットのコンテンツの場合、クライアントは全ての異なるコンテンツのＩフレーム位置データを格納したファイルを理解しなければならない。フォーマット数が多くなると、これは受信側にとって大きな負担となるため、送信側で異なるＩフレーム位置情報より、共通のＩフレーム位置情報生成手段８０１で共通のＩフレーム位置情報を生成する。これにより、各社のＨＤＤ記録フォーマット、ＤＶＤ－ＶＲ方式、あるいはＢＤ方式など異なる蓄積フォーマットであっても、簡単に、早送り、巻き戻し、スロー再生などの特殊再生することを実現する。
【０１２７】
このパケット化において、ＨＴＴＰは受信手段からのレンジリクエストまたはデータ取得コマンドを受けて前記ＡＶデータまたは前記暗号化モード情報のうち少なくとも一方を含んだペイロードデータを伝送する。このレンジリクエストまたはデータ取得コマンドは、前記送信側における前記ＡＶデータがＭＰＥＧの場合、ＭＰＥＧストリームにおける不連続発生連続性情報、前記ＡＶデータのファイル内におけるＭＰＥＧのＩピクチャまたはＰピクチャまたはＢピクチャの位置情報、或るＩピクチャから次のＩピクチャの間に存在するＰピクチャとＢピクチャの各個数または合計個数の内、少なくとも１つの情報を参照して実行する。ここで、ＭＰＥＧストリームにおける不連続発生情報とは、ＡＲＩＢ規格、ＡＲＩＢ－ＴＲ－Ｂ１４またはＡＲＩＢ－ＴＲ－Ｂ１４の第２編に記載されているＤＩＴ情報を元に生成することができる。このストリームの不連続点とは、たとえば、ＭＰＥＧのパーシャルＴＳの場合、ＭＰＥＧ－ＴＳストリームのシステムタイムベースの不連続が発生する点、たとえば、ＰＣＲが不連続になる点、または、パーシャルＴＳを構成するパケットの内のどれか１つのトランスポートパケットヘッダのcontinuity_counterの不連続が発生する点のことである。
【０１２８】
また、ＡＶデータのファイル内におけるＭＰＥＧのＩピクチャまたはＰピクチャまたはＢピクチャの位置情報は、前記ＡＶデータが複数の異なるファーマットであった場合にもオリジナルに持っている複数のＩピクチャまたはＰピクチャまたはＢピクチャの位置情報、前記ＭＰＥＧのＩピクチャまたはＰピクチャまたはＢピクチャの時刻情報より、複数の異なるファーマット間で共通なＩピクチャまたはＰピクチャまたはＢピクチャ位置情報を

生成し、この共通のＩピクチャまたはＰピクチャまたはＢピクチャ位置情報を用いて前記ＡＶデータのファイル内におけるＭＰＥＧのＩピクチャまたはＰピクチャまたはＢピクチャの位置情報、時刻情報の参照情報とする。これにより、たとえばＨＤＤに、異なる記録フォーマットで記録されているＭＰＥＧ－ＴＳファイルがあっても、リモート端末からは共通のＩまたはＰまたはＢピクチャの位置情報や時間情報で特定のピクチャに直接アクセスできるという大きなメリットがある。

【０１２９】

たとえば、図１３の一例の様に、パーシャルＴＳを記録したＨＤＤやＢＤディスクなどから、ＩまたはＰまたはＢピクチャの連続性およびファイル内での位置情報などを統一した「ピクチャ情報ファイル」にき出す。ネットワークを介して離れた場所に存在する端末からは、この統一されたピクチャ情報ファイルをバイト位置や時刻情報（timestamp)で参照することにより、異なるＴＳ記録フォーマットでも各ピクチャ位置をきめ細かに参照することができる。

【０１３０】

図１３において、“ｄｉｓｃｏｎｔ”はパーシャルＴＳの不連続点を示す１ビットのフラグである。たとえば、この値が“０”の時はパーシャルＴＳは連続であり、“１”の時は不連続を意味する。

【０１３１】

また、“ＩＰＢフラグ”は、２ビットのＩピクチャ、Ｐピクチャ、Ｂピクチャの識別フラグであり、その値が“００”の時はＩピクチャ、“０１”の時はＰピクチャ、“１０”の時はＢピクチャであることを示す。ここで、Ｉピクチャの場合は必ず記述が必要で、ＰまたはＢピクチャの場合は、オプションとし、必ずしも記述しなくてもよい。また、“Byte_position”は、Ｉピクチャ、Ｐピクチャ、およびＢピクチャの先頭のファイルにおけるバイト位置を３２ｂｉｔで示す。さらに、“PB_number”は、或るＩピクチャから次のＩピクチャまでの間に存在するＰピクチャとＢピクチャの合計数を５ビットで示す。“Ｔｉｍｅｓｔａｍｐ”は、Ｉピクチャ、Ｐピクチャ、Ｂピクチャの時刻情報で、それぞれのＭＰＥＧのＩピクチャまたはＰピクチャまたはＢピクチャを構成するタイムスタンプ付きＴＳ列の先頭など特定位置のＴＳのタイムスタンプ値を４０ビットに変換して使用する。それぞれのパラメータ、フラグの値の定義は、前記の組合せに限定されない。

【０１３２】

以上により、きめ細かやで綺麗なスロー再生や高速再生などのトリック再生が実現できる。なお、このピクチャ情報ファイルはリモート端末からローカル端末内の異なるファーマットで記録されたＭＰＥＧ－ＴＳファイル内のピクチャ位置を共通のファイル形式で見せることができるフィルタ機能として考えることができる。すなわち、独自のファイル形式でMPEG-TSを記録したAVデータファイルとその関連情報ファイルより、共通のピクチャ情報ファイルを生成することができる。

【０１３３】

本発明で用いる入力データの適用範囲として、サーバー型放送や各社の異なるＤＲＭ方式など一般のＤＲＭ対応のＡＶコンテンツをＤＴＣＰ－ＩＰを用いて伝送することが可能となる。

【０１３４】

また、第４の実施例の構成により、ＡＶコンテンツをＡＫＥや暗号処理を実装しない送受信装置による実装の場合にも、ＭＰＥＧのＩピクチャまたはＰピクチャまたはＢピクチャに効率よくアクセスできるという効果を得ることができる。

【０１３５】

さらに、本発明の別機能について説明する。図４のコンテンツバッファ４１３において、ＭＰＥＧ－ＴＳ信号に、たとえばリードソロモン方式のエラー訂正符号を付加した後、暗号化手段４１４で暗号化する。これにより、送受信機器間でＭＰＥＧ－ＴＳ信号をＤＴＣＰ方式により暗号化し、さらにエラー訂正符号を付加しリアルタイム伝送が可能となる。ここで、ＭＰＥＧ－ＴＳのヘッダー付加および伝送処理のパケット化手段をハードウェ

アで構成すると、本質的にソフトウェア処理に起因する送信パケットの送り残しや受信パケットの取りこぼしが発生しない。また、データ量の小さい一般データのパケット化はマイコンなど安価なプロセッサで処理できる。

【産業上の利用可能性】

【０１３６】

本願によれば、デジタル放送やＤＶＤディスクのコピー制限コンテンツを、コンテンツの著作権者によって設定されたコピー制御情報を継承しながらＩＰネットワークを用いて違法コピーを回避しつつ安全に伝送することが可能となる。たとえば、一般家庭において、１階の今にあるデジタルチュナーやＤＶＤレコーダから2回の寝室にあるディスプレイに映画などのプレミアムコンテンツを伝送することが可能となる。

【図面の簡単な説明】

【０１３７】

【図１】本願発明を適用するシステムの一例を示す図

【図２】認証と鍵交換にＤＴＣＰ方式を適用する場合のコンテンツ伝送手順の説明図

【図３】イーサネット（登録商標）を用いる一般家庭に適用した場合の一例の説明図

【図４】本願第１の発明および第２の発明のパケット送信手段のブロック図

【図５】本願第１の発明のプロトコルスタックによる説明図

【図６】本願第１の発明におけるＭＰＥＧ－ＴＳのイーサネット（登録商標）フレーム構成仕様の例を示す図

【図７】本願第３の発明におけるパケット送受信手段の構成を示すブロック図

【図８】本願第４の発明のパケット送受信手段の構成を示すブロック図

【図９】従来例における送信システムの説明図

【図１０】従来例における送信機器および受信機器の構成を示すブロック図

【図１１】従来例における鍵交換にＤＴＣＰ方式を適用する場合のコンテンツ伝送手順の説明図

【図１２】従来例における１３９５アイソクロナスパケットの構成例を示す図

【図１３】ピクチャ情報ファイルの構成を示す図

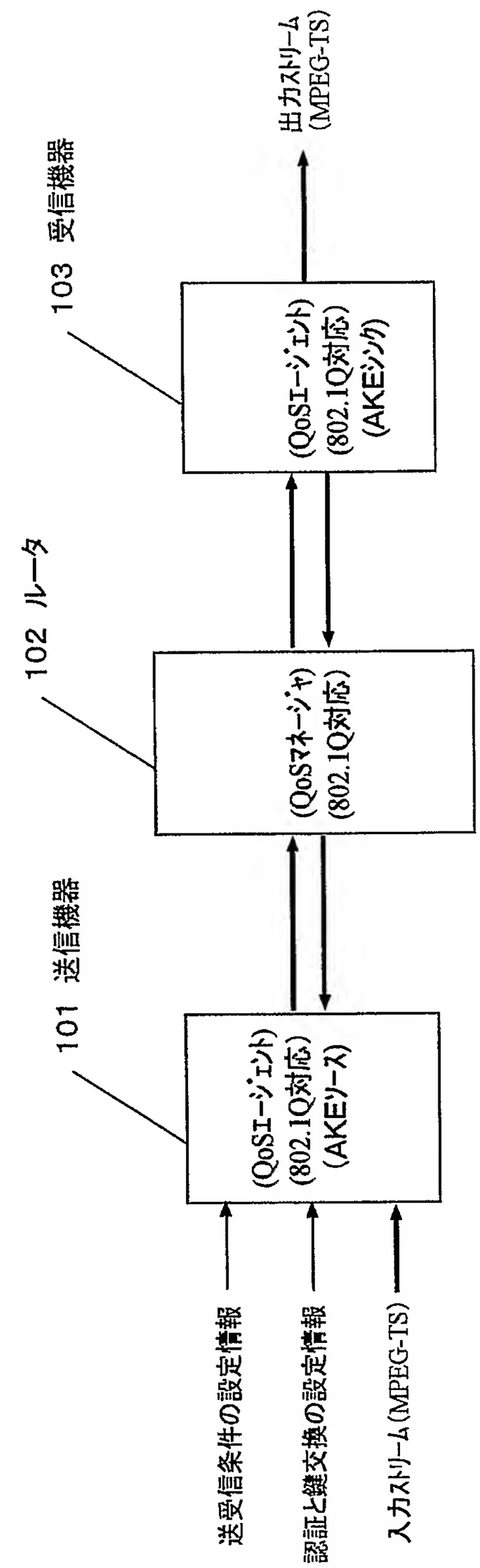
【符号の説明】

【０１３８】

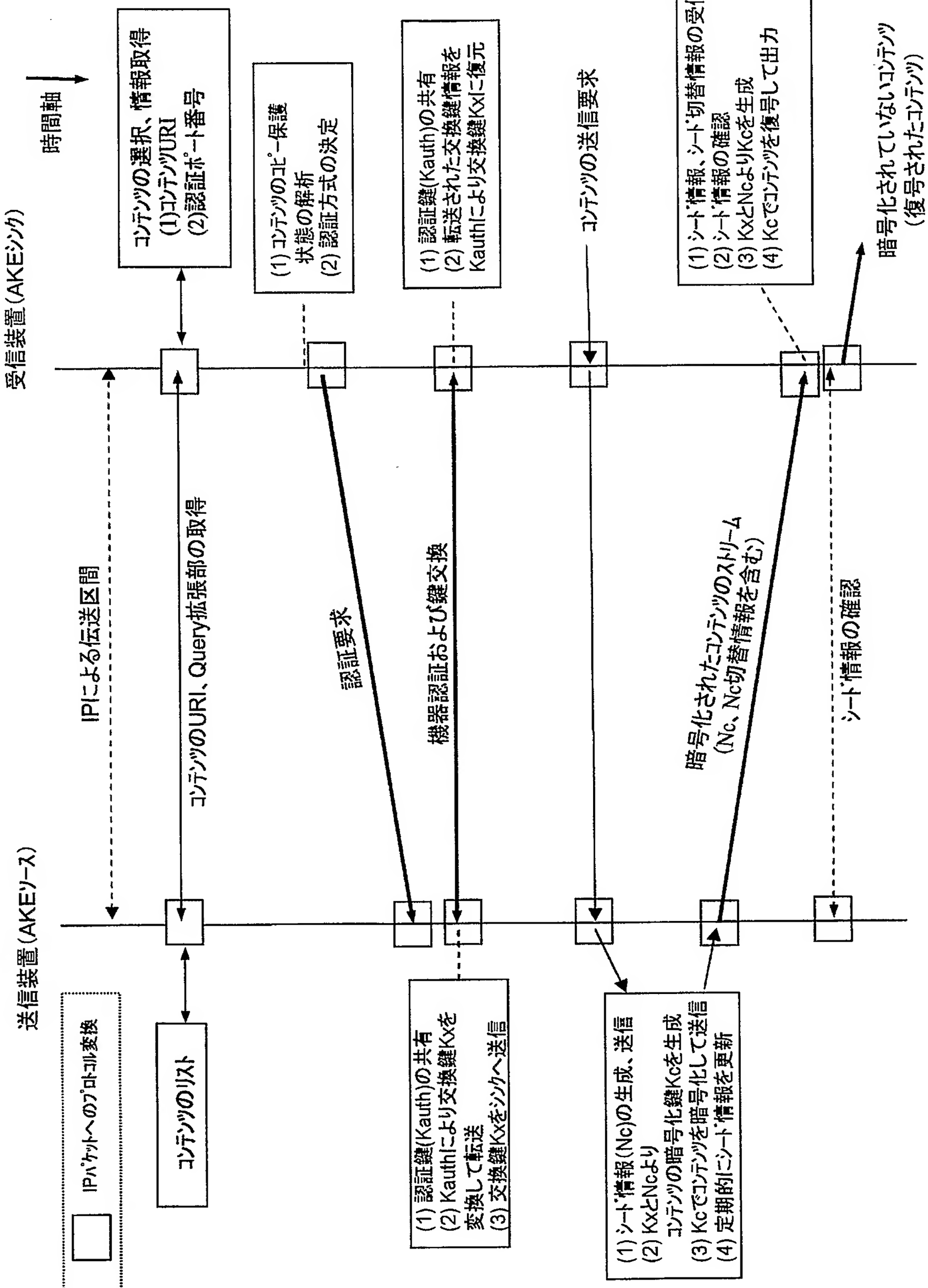
１０１　パケット送信機器
１０２　ルータ
１０３　パケット受信機器
４０１　パケット送信手段
４０２　ＴＳストリーム識別手段
４０３　送信条件の設定管理手段
４０４　ＤＲＭ設定管理手段
４０５　ＡＫＥ手段
４０６　パケット化手段
４０７　暗号化データ復号手段
４０８　フレーム化手段
４０９　フレーム受信手段
４１０　パケット受信手段
４１１　ＤＲＭコンテンツ購入決済手段
４１２　コンテンツメタ情報
４１３　コンテンツバッファ
４１４　暗号化手段
４１５　暗号化情報ヘッダー付加手段
４１６　ＨＴＴＰ／ＲＴＰヘッダー付加手段
４１７　送信条件の条件設定手段

４１８　復号化手段
７０１　蓄積手段
８０１　Ｉフレーム位置情報生成手段

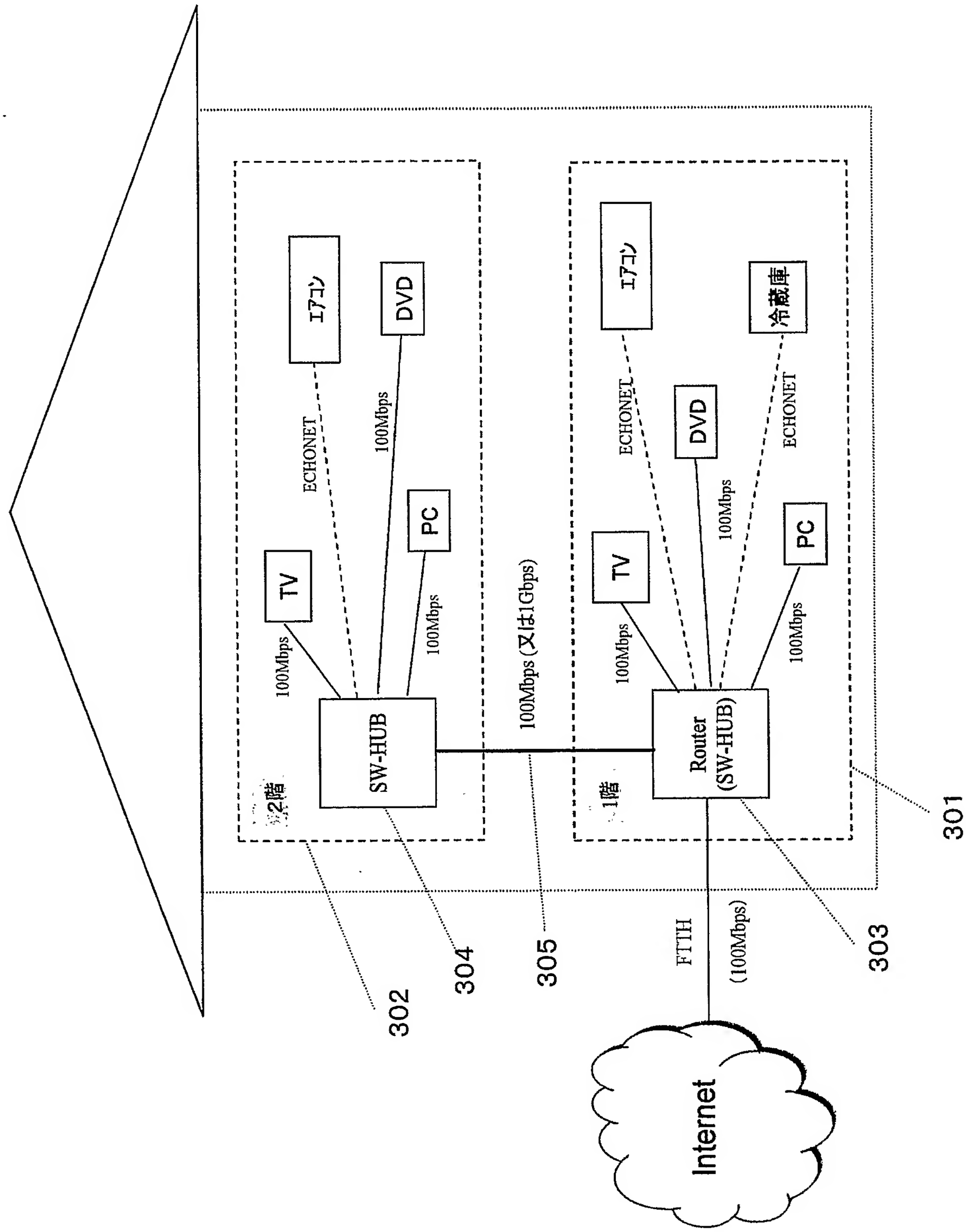
【書類名】図面
【図１】


103 受信機器
出力ストリーム
(MPEG-TS)
(QoSエージェント)
(802.1Q対応)
(AKEシンク)
102 ルータ
(QoSマネージャ)
(802.1Q対応)
101 送信機器
(QoSエージェント)
(802.1Q対応)
(AKEソース)
送受信条件の設定情報
認証と鍵交換の設定情報
入力ストリーム(MPEG-TS)

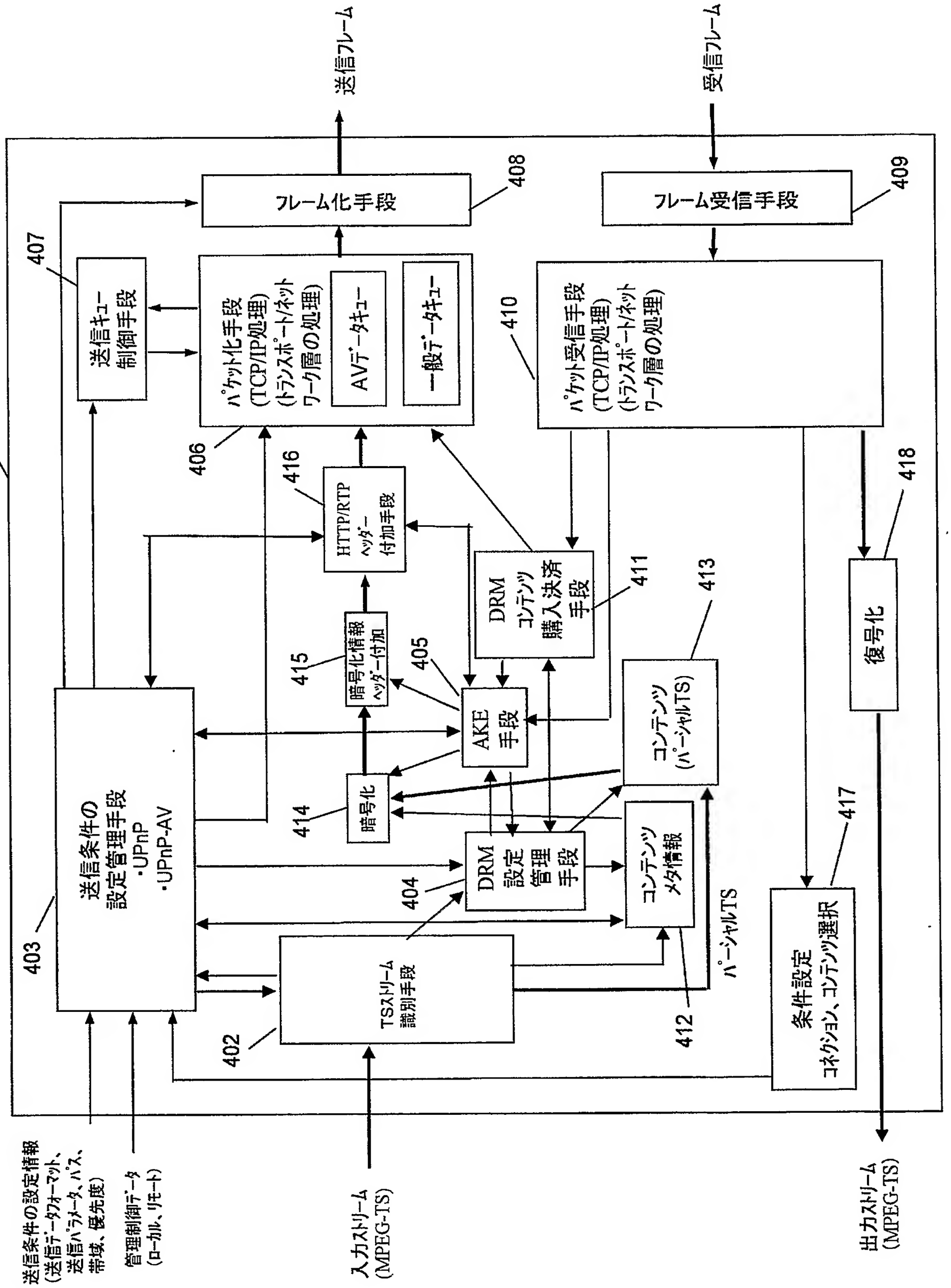
【図２】


送信装置(AKEシンク)
受信装置(AKEソース)
時間軸
IPパケットへのプロトコル変換
コンテンツのリスト
コンテンツの選択、情報取得
(1)コンテンツURI
(2)認証ポート番号
(1) コンテンツのコピー保護
状態の解析
(2) 認証方式の決定
(1) 認証鍵(Kauth)の共有
(2) 転送された交換鍵情報を
Kauthにより交換鍵Kxに復元
コンテンツの送信要求
(1) シード情報、シード切替情報の受信
(2) シード情報の確認
(3) KxとNcよりKcを生成
(4) Kcでコンテンツを復号して出力
暗号化されていないコンテンツ
(復号されたコンテンツ)
IPによる伝送区間
コンテンツのURI、Query拡張部の取得
認証要求
機器認証および鍵交換
暗号化されたコンテンツのストリーム
(Nc、Nc切替情報を含む)
シード情報の確認
(1) 認証鍵(Kauth)の共有
(2) Kauthにより交換鍵Kxを
変換して転送
(3) 交換鍵Kxをシンクへ送信
(1) シード情報(Nc)の生成、送信
(2) KxとNcより
コンテンツの暗号化鍵Kcを生成
(3) Kcでコンテンツを暗号化して送信
(4) 定期的にシード情報を更新

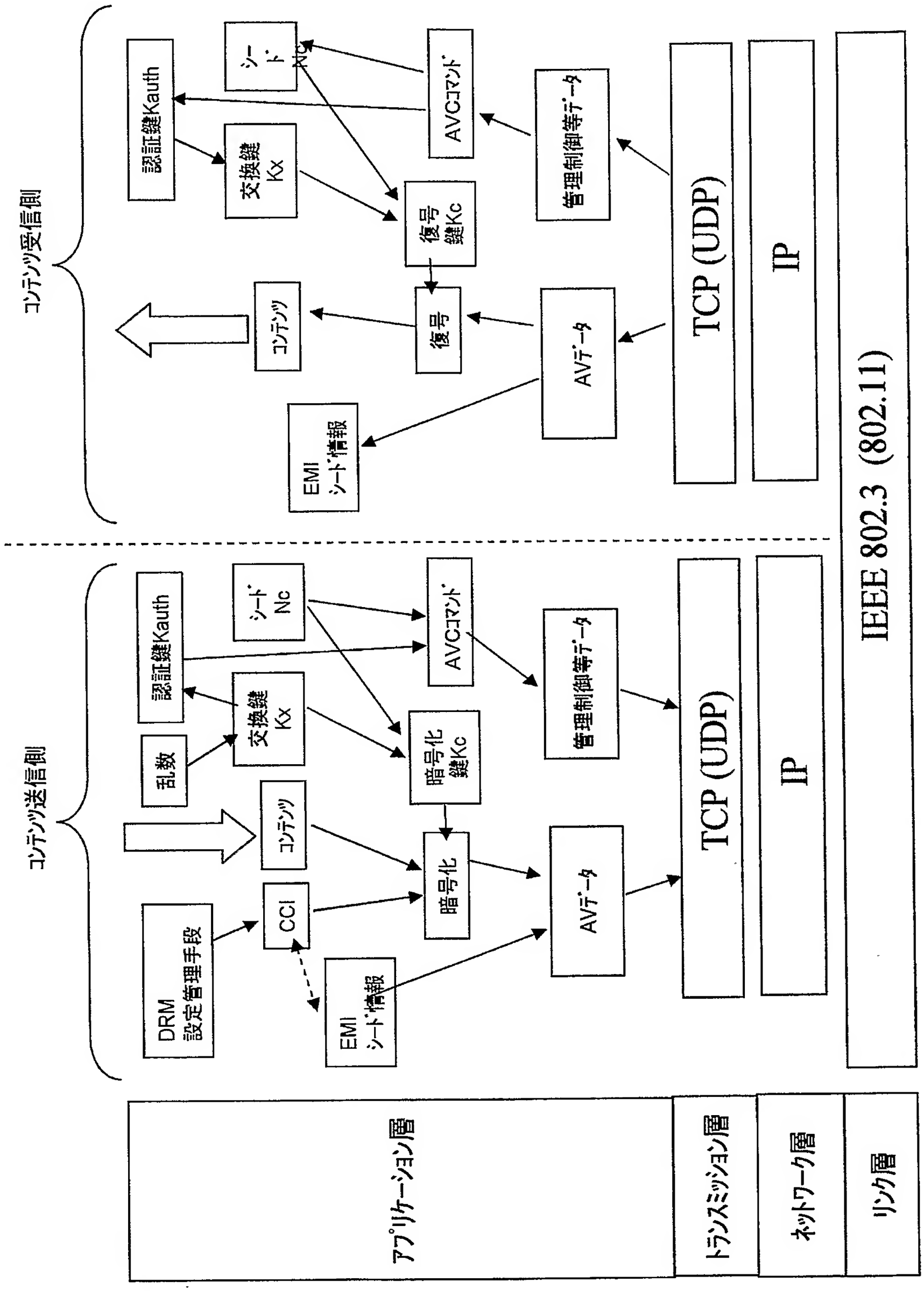
【図３】

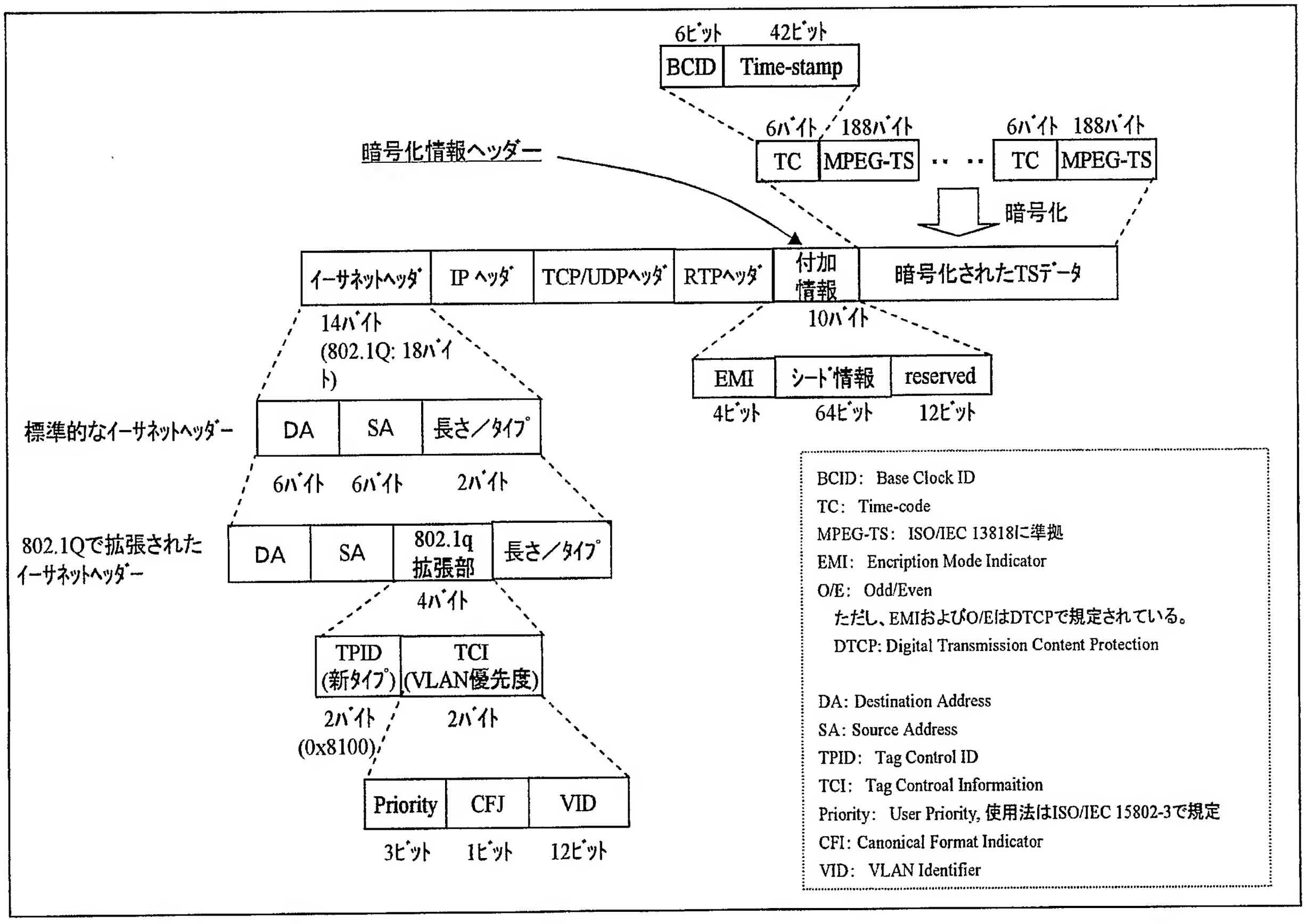

Internet
FTTH
(100Mbps)
Router
(SW-HUB)
SW-HUB
100Mbps (又は1Gbps)
100Mbps
ECHONET
TV
DVD
PC
エアコン
冷蔵庫
1階
2階
301
302
303
304
305

【図４】


送信フレーム
受信フレーム
フレーム化手段
408
フレーム受信手段
409
407
送信キュー制御手段
パケット化手段(TCP/IP処理)(トランスポート/ネットワーク層の処理)
AVデータキュー
一般データキュー
410
パケット受信手段(TCP/IP処理)(トランスポート/ネットワーク層の処理)
401
406
416
HTTP/RTPヘッダー付加手段
DRMコンテンツ購入決済手段
411
413
415
暗号化情報ヘッダー付加
405
AKE手段
コンテンツ(パーシャルTS)
復号化
418
414
暗号化
DRM設定管理手段
404
コンテンツメタ情報
パーシャルTS
403
送信条件の設定管理手段
・UPnP
・UPnP-AV
TSストリーム識別手段
402
412
417
条件設定
コネクション、コンテンツ選択
送信条件の設定情報
(送信データフォーマット、送信パラメータ、パス、帯域、優先度)
管理制御データ
(ローカル、リモート)
入力ストリーム
(MPEG-TS)
出力ストリーム
(MPEG-TS)

【図５】

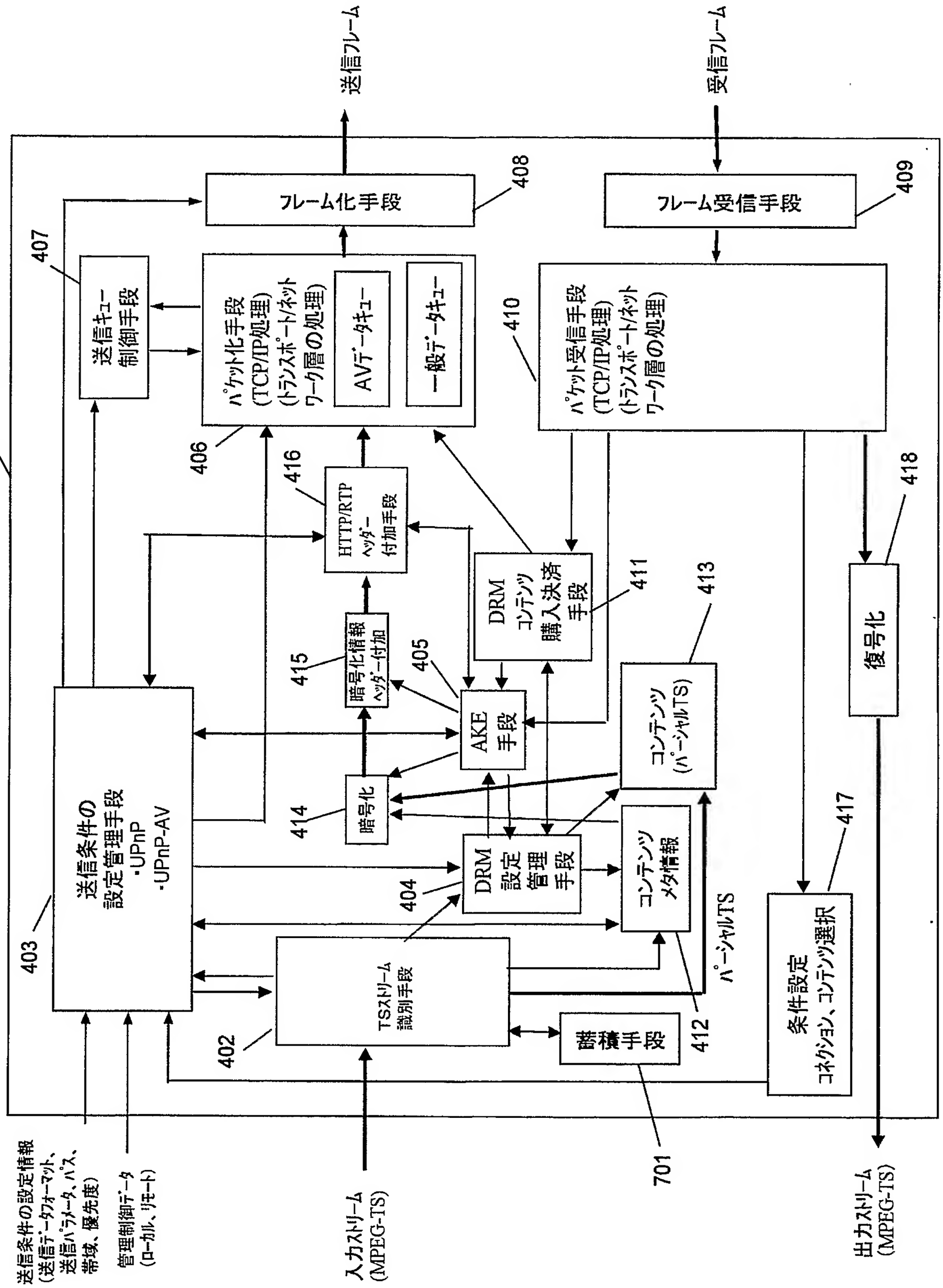

コンテンツ受信側
認証鍵Kauth
シード Nc
交換鍵 Kx
AVCコマンド
管理制御等データ
復号鍵Kc
コンテンツ
復号
AVデータ
TCP (UDP)
IP
IEEE 802.3 (802.11)
EMI シード情報
コンテンツ送信側
乱数
CCI
暗号化
暗号化鍵Kc
DRM 設定管理手段
アプリケーション層
トランスミッション層
ネットワーク層
リンク層
(OSIモデルによる説明)



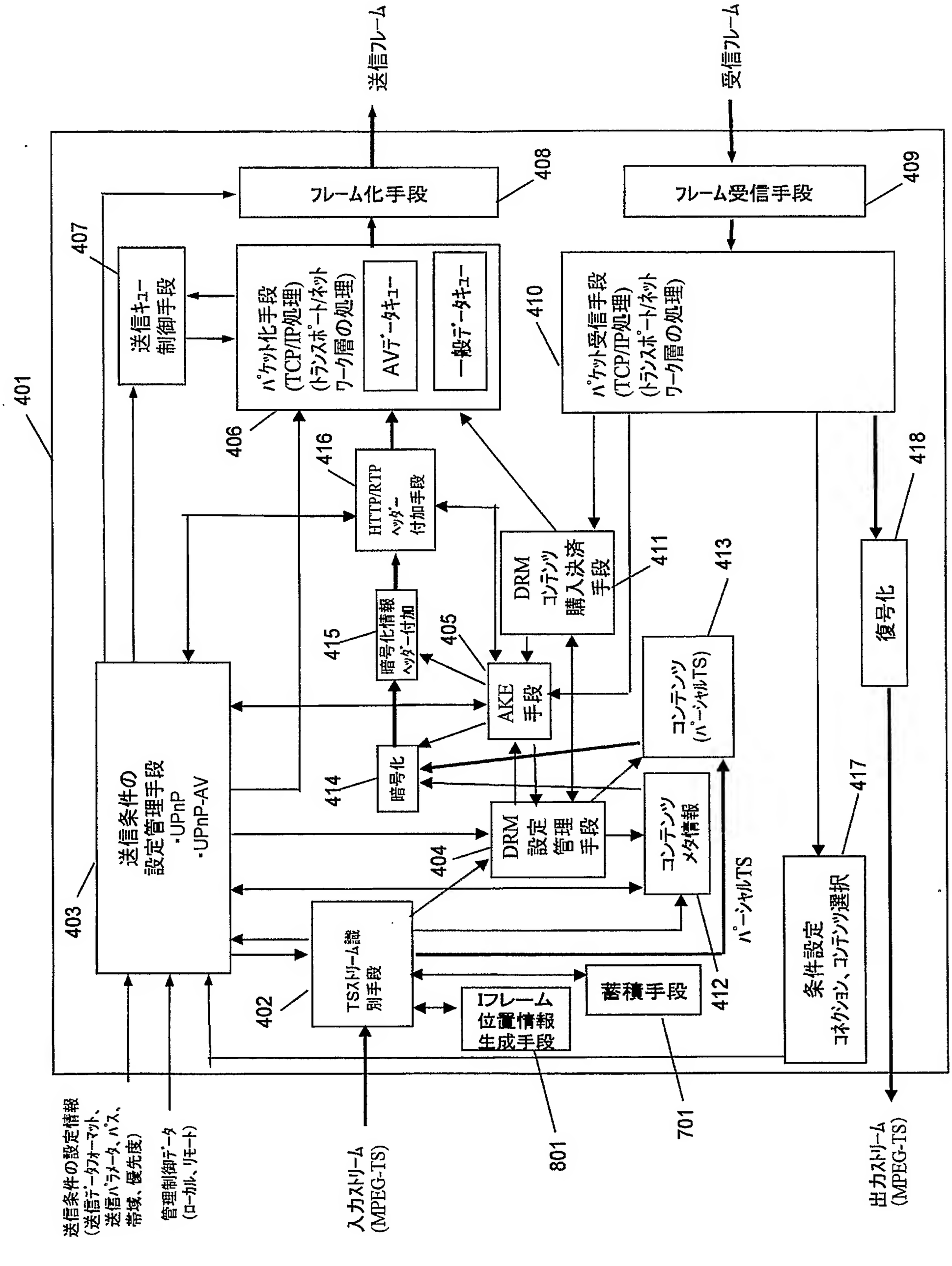
BCID: Base Clock ID
TC: Time-code
MPEG-TS: ISO/IEC 13818に準拠
EMI: Encription Mode Indicator
O/E: Odd/Even
ただし、EMIおよびO/EはDTCPで規定されている。
DTCP: Digital Transmission Content Protection

DA: Destination Address
SA: Source Address
TPID: Tag Control ID
TCI: Tag Controal Informaition
Priority: User Priority, 使用法はISO/IEC 15802-3で規定
CFI: Canonical Format Indicator
VID: VLAN Identifier

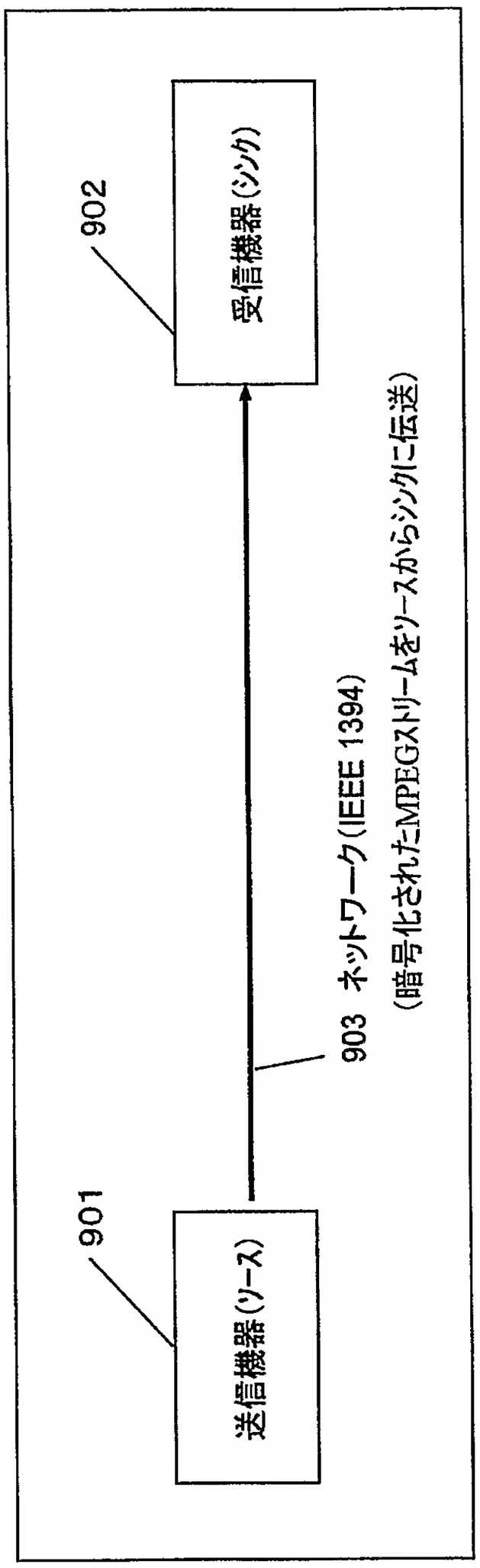
【図７】


送信フレーム
受信フレーム
401
フレーム化手段
408
フレーム受信手段
409
407
送信キュー制御手段
パケット化手段(TCP/IP処理)(トランスポート/ネットワーク層の処理)
AVデータキュー
一般データキュー
406
410
パケット受信手段(TCP/IP処理)(トランスポート/ネットワーク層の処理)
416
HTTP/RTPヘッダー付加手段
415
暗号化情報ヘッダー付加
405
DRMコンテンツ購入決済手段
411
413
418
復号化
AKE手段
コンテンツ(パーシャルTS)
414
暗号化
403
送信条件の設定管理手段
・UPnP
・UPnP-AV
DRM設定管理手段
404
コンテンツメタ情報
パーシャルTS
417
条件設定
コネクション、コンテンツ選択
TSストリーム識別手段
402
蓄積手段
412
701
送信条件の設定情報(送信データフォーマット、送信パラメータ、パス、帯域、優先度)
管理制御データ(ローカル、リモート)
入力ストリーム(MPEG-TS)
出力ストリーム(MPEG-TS)

【図８】


送信フレーム
受信フレーム
フレーム化手段
408
フレーム受信手段
409
407
送信キュー制御手段
パケット化手段(TCP/IP処理)(トランスポート/ネットワーク層の処理)
AVデータキュー
一般データキュー
410
パケット受信手段(TCP/IP処理)(トランスポート/ネットワーク層の処理)
401
406
416
HTTP/RTPヘッダー付加手段
DRMコンテンツ購入決済手段
411
413
415
暗号化情報ヘッダー付加
405
AKE手段
ユニーク(パーシャルTS)
復号化
418
414
暗号化
DRM設定管理手段
404
コンテンツメタ情報
417
403
送信条件の設定管理手段
・UPnP
・UPnP-AV
TSストリーム識別手段
402
Iフレーム位置情報生成手段
蓄積手段
412
パーシャルTS
条件設定
コネクション、コンテンツ選択
送信条件の設定情報(送信データフォーマット、送信パラメータ、パス、帯域、優先度)
管理制御データ(ローカル、リモート)
入力ストリーム(MPEG-TS)
801
701
出力ストリーム(MPEG-TS)

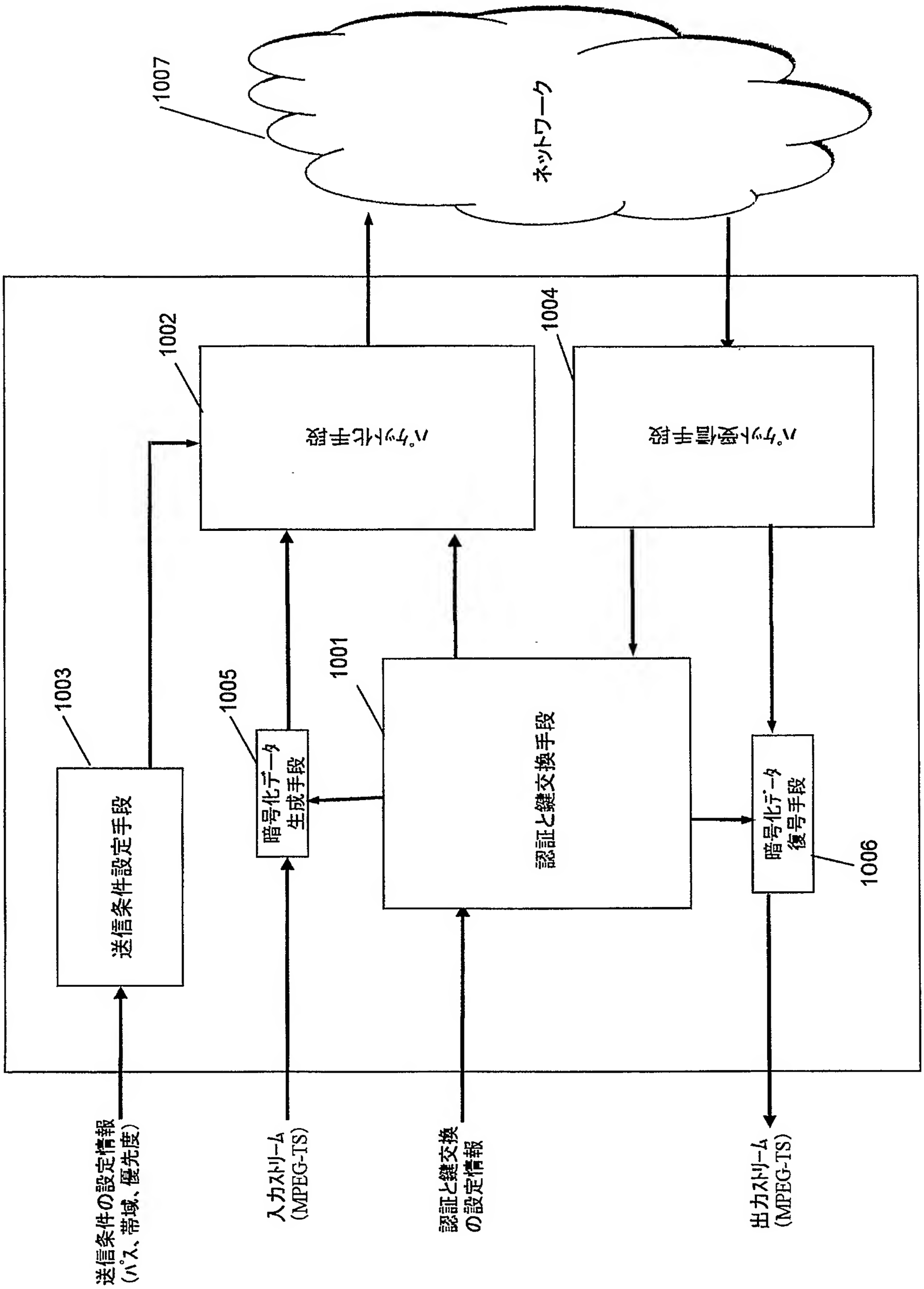
【図９】



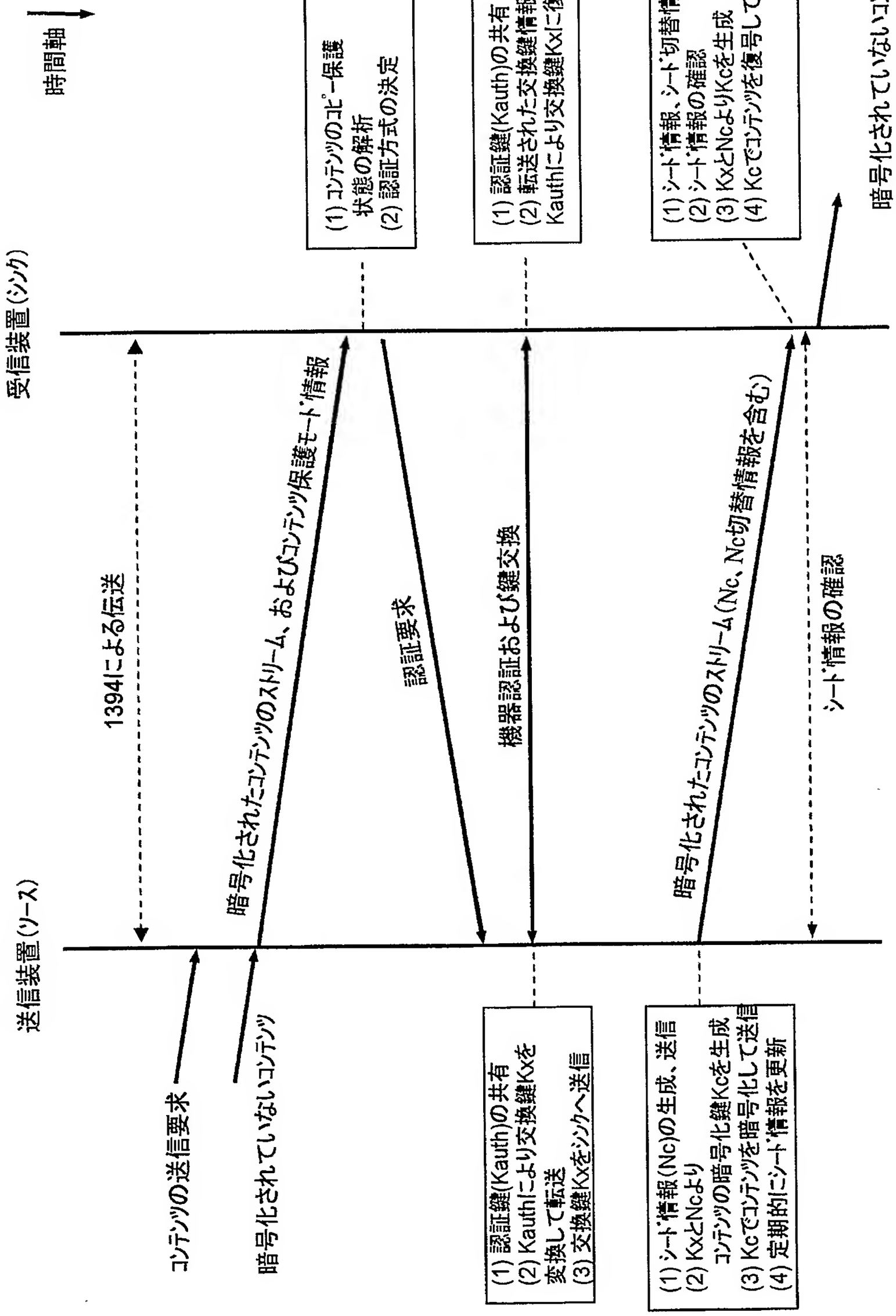
送信機器(ソース)の例	受信機器(シンク)の例	コンテンツ伝送における暗号化
DVHS	DVHS	MPEG-TSにDTCP方式によるコンテンツ保護を実施
HDDレコーダ	HDDレコーダ	
1394搭載STB	1394搭載STB	
1394搭載ディジタルTV	1394搭載ディジタルTV	

IEEE 1394においてDTCPを用いたMPEGストリームの伝送

【図１０】

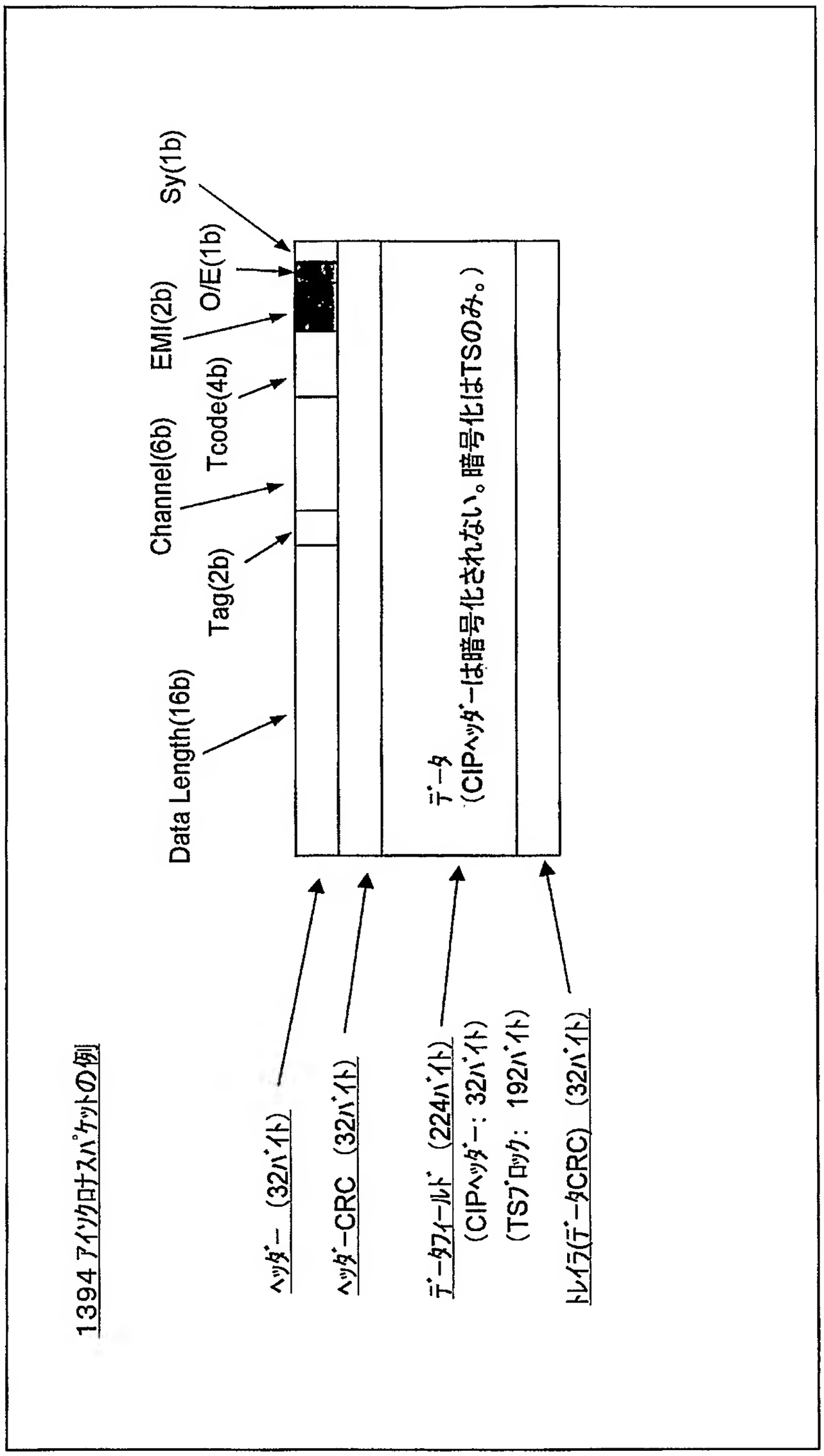

ネットワーク
1007
1002
ﾊﾟｹｯﾄ化手段
1004
ﾊﾟｹｯﾄ受信手段
1003
送信条件設定手段
1005
暗号化ﾃﾞｰﾀ
生成手段
1001
認証と鍵交換手段
暗号化ﾃﾞｰﾀ
復号手段
1006
送信条件の設定情報
(ﾊﾟｽ、帯域、優先度)
入力ｽﾄﾘｰﾑ
(MPEG-TS)
認証と鍵交換
の設定情報
出力ｽﾄﾘｰﾑ
(MPEG-TS)

【図１１】

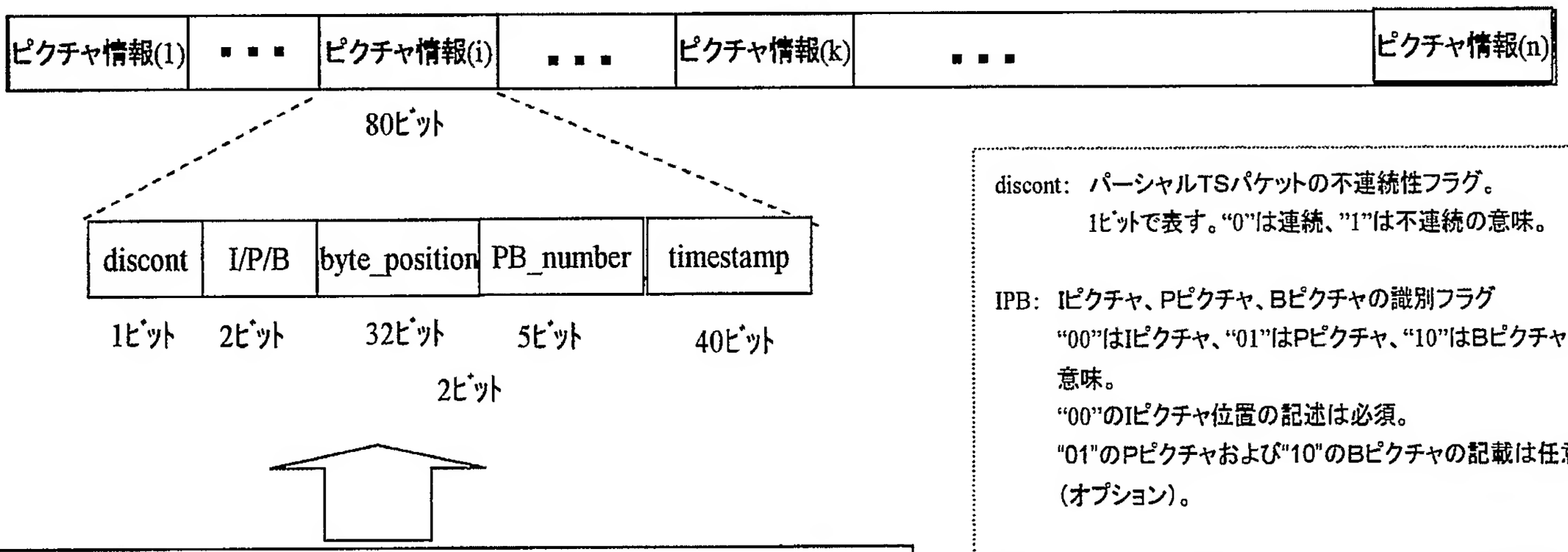


IEEE 1394においてDTCPを用いた暗号化ストリーム伝送手順(従来技術)

【図１２】


1394アイソクロナスパケットの例
ヘッダー（32バイト）
ヘッダーCRC（32バイト）
データフィールド（224バイト）
（CIPヘッダー：32バイト）
（TSプロック：192バイト）
トレイラ(データCRC)（32バイト）
Data Length(16b)
Tag(2b)
Channel(6b)
Tcode(4b)
EMI(2b)
O/E(1b)
Sy(1b)
データ
(CIPヘッダーは暗号化されない。暗号化はTSのみ。)

ピクチャ情報ファイル(PIF: Picture Information File)の構成



パーシャルTSを記録したHDDや
BDディスクなどから、I／P／Bピクチャの連続性、位置情報、時刻情報などを統一した「ピクチャ情報ファイル」に書き出す。ネットワークを介して離れた場所に存在する端末からは、このピクチャ情報ファイルを参照することにより、異なるTS記録フォーマットでも各ピクチャ位置が参照できる。これにより、きめ細かなスローや高速再生などが実現できる。

discont: パーシャルTSパケットの不連続性フラグ。
1ビットで表す。"0"は連続、"1"は不連続の意味。

IPB: Iピクチャ、Pピクチャ、Bピクチャの識別フラグ
"00"はIピクチャ、"01"はPピクチャ、"10"はBピクチャの意味。
"00"のIピクチャ位置の記述は必須。
"01"のPピクチャおよび"10"のBピクチャの記載は任意(オプション)。

Byte_position: Iピクチャ、Pピクチャ、Bピクチャの先頭のファイルにおけるバイト位置。32bitで表す。

PB_number: 或るIピクチャから次のIピクチャまでの間に存在するPピクチャとBピクチャの合計数。5bitで表す

Timestamp: Iピクチャ、Pピクチャ、Bピクチャの時刻情報。
40bitで表す。

【書類名】要約書
【要約】
【課題】デジタル放送やサーバー型放送などの著作権保護されたＭＰＥＧコンテンツを、そのＲＭＰＩなどデジタル著作権情報を継承しつつ、ＩＰネットワークを用いて伝送する手段を実現する。また、ＲＭＰやネットＤＲＭに対応していない受信機においても視聴を可能とする。
【解決手段】本願発明によるパケット送信手段は、ＡＶデータとデジタル著作権管理情報などを夫々入力するデータ入力手段と、デジタル著作権情報をＤＴＣＰ－ＩＰ伝送の送受信条件に変換する手段と、暗号化または暗号化情報ヘッダー付加の実行を行う暗号化データ生成手段と、パケットヘッダー付加手段とを具備するパケット送受信手段において、暗号化データ生成手段は認証手段と暗号化手段と暗号化情報ヘッダー付加手段を具備する。また、異なるフォーマットに対して共通のＩフレーム位置情報を生成する手段を具備するため、複数の蓄積フォーマットに対して効率のよい特殊再生を実現する。
【選択図】　図４

特願２００４－２６１０３３

出　願　人　履　歴　情　報

識別番号　［０００００５８２１］

１．変更年月日　１９９０年　８月２８日
［変更理由］　新規登録
住　所　大阪府門真市大字門真１００６番地
氏　名　松下電器産業株式会社